НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ УКРАЇНИ
«КИЇВСЬКИЙ ПОЛІТЕХНІЧНИЙ ІНСТИТУТ
імені ІГОРЯ СІКОРСЬКОГО»

Інститут телекомунікаційних систем

Кафедра Телекомунікаційних систем

«На правах рукопису»
УДК _____

«До захисту допущено»
Завідувач кафедри
_____ Л.О. Уривський
«___»_____20__ р.

Магістерська дисертація

на здобуття ступеня магістра

зі спеціальності 172 Телекомунікації та радіотехніка

на тему: «Квантові однофотонні системи зв'язку»

Виконав:
студент ІІ курсу, групи ТС-61м
Григорчук Андрій Олександрович _____

Керівник:
Доктор технічних наук, професор,
Трубін Олександр Олексійович _____

Рецензент:
Доктор технічних наук, доцент,
Манько Олександр Олексійович _____

Засвідчую, що у цій магістерській дисертації немає запозичень з праць інших авторів без відповідних посилань.
Студент _____

Київ – 2018 року

Національний технічний університет України
«Київський політехнічний інститут імені Ігоря Сікорського»
Інститут телекомунікаційних систем
Кафедра Телекомунікаційних систем

Рівень вищої освіти – другий (магістерський) за освітньо-науковою програмою

Спеціальність (спеціалізація) – 172 «Телекомунікації та радіотехніка» (172.3620.1 «Телекомунікаційні системи та мережі»)

ЗАТВЕРДЖУЮ
Завідувач кафедри
_____ Л.О. Уривський
«___»_____20__ р.

ЗАВДАННЯ
на магістерську дисертацію студенту
Григорчуку Андрію Олександровичу

1. Тема дисертації «Квантові однофотонні системи», науковий керівник дисертації Трубін Олександр Олексійовчи, д.т.н., професор, затверджені наказом по університету від «06» квітня 2018 р. №1105-с

2. Термін подання студентом дисертації _____

3. Об’єкт дослідження архітектура квантової одно фотонної мережі

4. Предмет дослідження одиночні фотони

5. Перелік завдань, які потрібно розробити

- Огляд принципів побудови однофотонних систем зв’язку;
- Аналіз структури, принципів функціювання, застосування, переваг та недоліків протоколів передачі фотонів;
- Оптимальна схема мережі та протоколи, які забезпечують конфіденційність передачі;
- Можливість виявлення наявності в каналі перехоплювачів в каналі звязку;
- Прилад для виявлення перехоплювачів інформації в лінії зв’язку.

6. Орієнтовний перелік графічного (ілюстративного) матеріалу
Плакат №1 «Тема, мета та завдання магістерської дисертації»
Плакат №2 «Постановка задачі»
Плакат №3 «Квантове розподілення ключа»
Плакат №4 «Протоколи кодування»
Плакат №5. «Опис роботи та застосування квантового рефлектометра»
Плакат №6. «Висновки»

7. Орієнтовний перелік публікацій

Заявка на патент від

8. Дата видачі завдання 10 вересня 2016 р.

Календарний план

№ з/п	Назва етапів виконання магістерської дисертації	Термін виконання етапів магістерської дисертації	Примітка
1	Огляд науково-технічної літератури, визначення недоліків досліджень та мети дипломної роботи	01.09.2016- 31.12.2016	
2	Вивчення квантових властивостей фотонів та однофотонних пристроїв для систем звязку	10.01.2017 - 29.02.2017	
3	Поглиблене вивчення квантових технологій зв'язку в курсе «Перспективні технології в телекомунікаційних системах»	01.03.2017 – 30.07.2017	
4	Вивчення станів фотонів та огляд пристроїв однофотонної мережі	01.08.2017 – 31.10.2017	
5	Огляд і аналіз методів кодування одиночних і заплутаних фотонів	01.11.2017 – 30.01.2018	
6	Розробка методів зондування мережі з використанням запутаних фотонів	01.02.2018 – 31.03.2018	
7	Використання методів зондування за допомогою заплутаних фотонів, розрахунки можливих втрат в середовищі передачі інформації	01.04.2018 – 30.04.2018	
8	Узагальнення результатів досліджень, підготовка звіту. Подання роботи та її захист	01.05.2018 - 20.05.2018	

Студент А. О. Григорчук

Науковий керівник дисертації О. О. Трубін

РЕФЕРАТ

Темою магістерської дисертації є квантовіодно фотонні системи зв’язку.

Робота містить 101 сторінку, зокрема 36 ілюстрацій, 5 таблиць та 20 джерел інформації.

Тема магістерської дисертації є актуальною, так як через зростаючі вимоги до конфіденційності інформації, вимагають від телекомунікаційних систем повного захисту переданої інформації.

Мета дисертації полягає в створенні приладу, який зможе забезпечити виявлення в лінії звязку прослуховувачів інформації, яка передається.

Об’єктом дослідження є архітектура квантової одно фотонної мережі. Предметом дослідження є одиночні фотони.

При виконанні роботи розроблялась блок-схема квантового однофотонного рефлектора.

У дисертації був запропонований прилад, який надає можливість виявити в лінії передачі сторонніх осіб, що намагаються прослухати передану інформацію.

ABSTRACT

The theme of the master's thesis is quantumone photonic communication systems.

The work contains 101 pages, in particular 36 illustrations, 5 tables and 20 sources of information.

The topic of the master's thesis is relevant, because due to increasing requirements for the confidentiality of information, telecommunication systems require full protection of the transmitted information.

The purpose of the dissertation is to create a device that can provide identification of the listeners of the information being transmitted in the communication line.

The object of research is the architecture of a quantum one photon network. The subject of the study is single photons.

When performing the work, a block diagram of a quantum single-photon reflector was created.

In the dissertation was proposed device, which provides an opportunity to detect in the transmission line of third parties trying to listen to the information transmitted.

РЕФЕРАТ

Темой магистерской диссертации является квантовиодно фотонные системы связи.

Работа содержит 101 страницу, в том числе 36 иллюстраций, 5 таблиц и 20 источников информации.

Тема магистерской диссертации является актуальной, так как через возрастающие требования к конфиденциальности информации, требуют от телекоммуникационных систем полной защиты передаваемой информации.

Цель диссертации заключается в создании прибора, который сможет обеспечить выявление в линии связи прослушивания информации, которая передается.

Объектом исследования является архитектура квантовой однофотонной сети. Предметом исследования является одиночные фотоны.

При выполнении работы разрабатывалась блок-схема квантового однофотонного рефлектора.

В диссертации был предложен прибор, который позволяет выявить в линии передачи посторонних лиц, пытающихся прослушать передаваемую информацию.

ЗМІСТ

ПЕРЕЛІК СКОРОЧЕНЬ

КРК – квантове розподілення ключів;

ВК – виправлений ключ;

ПВК – перехоплений виправлений ключ;

ДОФ – джерело одиночних фотонів;

ІЧ – інфрачервоне;

ФЕП – фотоелектронний перемножував;

ЛФД – лавинний фотодіод;

ВАХ – вольт-амперна характеристика;

ЯП – ячейка Поккельса;

ПСД – поляризаційний світло дільник;

ФМ – фазовий модуль;

СР – короткоперіодичні надрешітки;

НЧ – низькі частоти.

ВСТУП

Розвиток суспільства і обмін інформацією – взаємопов'язані складові прогресу. Обсяг та надійність передачі є ключем до розвитку країни. Під час розвитку стрімкого розвитку технологій неможливо уявити життя без засобів передачі інформації, не кажучи вже про науку та управлінську діяльність. Спокон віків людство потребувало надійні та конфіденційні засоби передачі інформації.

Телекомунікаційні системи проходять шлях еволюції кожного дня, починаючи від звукових та візуальних пристроїв і закінчуючи системами автоматичного обміну, які забезпечують обмін інформацією на необмежені відстані в межах Землі.

Майже кожен в наш час отримує доступ до переліку необхідних послуг, починаючи з передачі текстових повідомлень і закінчуючи медіа контентом. Провайдери, які забезпечують доступ до мережі Intertet, мають великі розповсюджені мережі. Основною задачею провайдерів є забезпечення якості зв'язку, та в першу чергу конфіденційності переданої інформації.

Конфіденційно-орієнтований підхід до побудови мережі передбачає постановку вирішення задачі забезпечення передачі інформації, яка буде повністю захищена від прослуховування. В даній роботі будуть розглядатися методи передачі інформації з повним захистом від сторонніх користувачів шляхом використання протоколів квантових систем передачі.

В наш час телекомунікаційні системи зв'язку досягаюсь конфіденційності за рахунок використання стандартних протоколів та кодувань інформації. Задача реалізації конфіденційності в даній роботі вирішується з використанням квантових частинок світла – фотонів.

РОЗДІЛ 1. КВАНТОВА КРИПТОГРАФІЯ

1.1 Змішані стани

Під час проведення перших дослідів над елементарними частинками було виявлено, що їх поведінку доволі важко описати, ґрунтуючись на вже існуючих представленнях про фізичні явища. Це призвело до того, що при формулюванні нових законів, описуючих поведінку елементарних частинок, цю частину фізики почали називати квантовою теорією, а ту частину фізики яка вже склалась – класичною.

Одна з головних відмінностей класичної фізики від квантової теорії проявляється вже в визначенні квантової частинки і її стану. Представлення частинки як тіла, що має визначені координати, розміри і масу, виявилось зовсім неправильним, так як для деяких таких частинок не вдавалося навіть зрозуміти, в якій точці простору вони знаходяться. Проте виявилось можливим передбачити поведінку таких частинок. Однак складність полягала в тому, що для пояснення цієї поведінки потрібно відмовитись від традиційних фізичних характеристик. Це призвело до того, що стан будь-якої елементарної частинки (або системи) стало представлятися за допомогою "хвильової функції" - принципіально нового об'єкта квантової картини світу.

Для початку потрібно ввести поняття чистого квантового стану. Таким станом будемо називати вектор в гільбертовому просторі H з одиничною нормою. Під нормою вектора розуміється корінь з його скалярного квадрата $\|\psi\| = \sqrt{\langle\psi|\psi\rangle}$ $\psi \in$ H .

Для кожного чистого квантового стану $|\psi\rangle$ можна визначити відповідний йому оператор $\rho_\psi = |\psi\rangle\langle\psi|$, який називається оператором щільності. Даний оператор має ранг 1 і дорівнює одиниці, і він діє як проектор на чистий стан $|\psi\rangle$.

За допомогою операторів щільності вводиться загальне поняття квантового стану[1]. Змішаним квантовим станом називається статистична суміш декількох чистих станів:

$$\rho = \sum_\iota \rho_\iota |\psi_\iota\rangle \langle\psi_\iota|, \rho_\iota \geq 0 \ \forall_\iota, \ \sum_\iota \rho_\iota = 1. \tag{1.1}$$

Очевидним є те що слід змішаного стану дорівнює одиниці. Його позитивна визначеність визначається таким чином:

$$\langle\varphi|\rho|\varphi\rangle = \sum_\iota \rho_\iota |\langle\varphi|\psi\rangle|^2 \geq 0 \quad \forall_{|\varphi\rangle} \in H \tag{1.2}$$

Далі, будь-який ермітів оператор A, має спектральне розкладання:

$$\mathrm{A} = \sum_\iota \lambda_\iota |\lambda_\iota\rangle\langle\lambda_\iota| \tag{1.3}$$

де власні значення λ_ι речові, а власні вектори $|\lambda_\iota\rangle$ нормовані і ортогональні. Це означає, що в будь-який позитивний ермітів оператор з одиничним слідом можна назвати оператором щільності деякого квантового стану: з позитивної визначеності отримуємо позитивність всіх власних значень, а з умови одиничного сліду – сума власних значень дорівнює одиниці, з цього випливає, що така комбінація може трактуватись як статистична суміш. Це приводить до загального визначення квантового стану: позитивний ермітів оператор в гільбертовому просторі H з одиничним слідом.

Квантові стани складають безліч операторів в просторі над H. Множину квантових станів прийнято позначати S(H). Крайніми точками цих станів є чисті квантові стани, які описуються операторами ранга 1.

Ключовий закон квантової механіки – рівняння Шредінгера, яке описує зміну квантових станів в часі. Традиційно в квантовій механіці рівняння описується:

$$\iota\hbar\frac{d|\psi\rangle}{dt} = H|\psi\rangle \tag{1.4}$$

де $\hbar$ - стала Планка і приблизно дорівнює $1{,}054 \cdot 10^{-34}$.

Ермітів оператор H називається гамільтаніоаном системи і саме він впливає на її еволюцію.

Відповідність між ермітовими і унітарними операторами:

$$U = e^{\iota H} \tag{1.5}$$

Рівняння Шредінгера може бути записано в вигляді[2]:

$$|\psi'\rangle = U|\psi\rangle.$$

В подальшому саме цей вид рівняння Шредінгера приймається як найбільш прийнятний, він означає, що будь-яка еволюція квантової системи може бути представлена як дія унітарного перетворення.

1.1.1 Квантові вимірювання

Відмінність вимірів в квантовій теорії і класичній фізиці є те, що у випадку виміру квантової системи її початкове значення змінюється.

В будь-якому експерименті можна виділити дві стадії: підготовку стану та його вимірювання. Вимірювання не повинно давати точно очікуваний

результат, в загальних випадках результат виміру – набір вихідних даних з деякими очікуваннями.

Неточні виміри. Досить часто на практиці зустрічається ситуація, коли результат вимірювань відомий неточно, тобто відомо, що результат відповідає деяким значенням, який належить деякій множині значень. Це трапляється через шум показників приладу, що в свою чергу не дає можливості достигнути необхідної точності. Така ситуація завжди має місце при вимірі неперервних змінних. В такому випадку результату виміру g_ι відповідає оператор $G_\iota = \sum_{S_\iota \epsilon \gamma_\iota} |S_\iota\rangle \langle S_\iota|$, а ймовірність виміру g_ι представляється виразом[3]:

$$\mathrm{p}_\iota = Tr\{G_\iota \rho\} \tag{1.6}$$

де ρ – оператор щільності вимірюваної системи.

Після виміру система переходить в змішаний стан з оператором щільності.

Узагальнені виміри – в загальному випадку набору результатів вимірів $\{g_\iota\}$ відповідає набір позитивних операторів $\{G_\iota\}$, виконується розкладання одиниці $\sum_\iota G_\iota = 1$.

Вимір називається узагальненим і міра ймовірності є позитивно-операторною мірою. Отримання будь-якого результату виміру не завжди може надати однозначну відповідь про стан системи.

1.2 Оптичне поле

Фізичний об’єкт за допомогою якого реалізується квантова криптографія – оптичне поле, або електромагнітне поле оптичного діапазону. Послаблення або збудження оптичного поля може відбуватись порціями, а саме фотонами,

енергія фотона $\hbar\omega$, де ω – частота, $\hbar = h/2\pi$ [3]. Оптичне поле представляється у вигляді набору його складових, а саме мод поля.

Мода поля - це стабільний стан електромагнітного поля всередині світловоду. Є одним з рішень рівнянь Максвелла для певної, заданої умовами структури. Моди поля в вільному просторі з граничними умовами на деякій поверхні, наприклад куб L^3- найпростіший випадок. В такому випадку поле представлено в вигляді разкладу по плоских бігучих хвилях. Під час розкладання кожна мода характеризується:

1) хвилевим вектором, який визначає направленість розповсюдження і частоту коливать. Проекції хвилевого вектора на грані куба кратні $2\pi/L$, згідно до умови періодичності[3].

2) направлення коливань вектора напруженості Е. Зважаючи на силу поперечного характера електромагнітної хвилі, існує два незалежних направлення коливань напруженості Е, які задаються двома одиничними векторами поляризації, які лежать в площині, перпендикулярній хвилевому вектору[3]. Нормуючий множник, вибраний таким чином, щоб амплітуди були безрозмірними. В класичній електродинаміці ці амплітуди є комплексними числами. В квантовій теорії оператори еквівалентні комутаційним співвідношенням для системи гармонічних осциляторів, які в свою чергу відповідають своїй моді.

Поле еквівалентного набору гармонічних осциляторів, повна енергія яких виражається: $H_n = \frac{1}{8\pi}\int((E^{(-)}(r,t)\cdot E^{(+)}(r,t)) + \text{ерм.опір.})dV = \sum_v \hbar\omega(a_v + a_v + 1/2)$, де інтегрування виконується по об'єму квантування поля L^3, a_v – оператори породження або знищення фотонів.

Оптичне поле – моди плоскої біжучої хвилі, варто відмітити, що реальні об'єкти з якими мають справу в експериментах відрізняються один від одного поляризаційним індексом.

Світловий пучок з заданим хвильовим вектором еквівалентний двом гармонічним осциляторам або модам, відповідним двом ортогонально поляризованим коливанням електромагнітного поля.

1.2.1 Однофотонні оптичні імпульси

У випадку коли відомо, що об’єкт має один фотон, стан його задається суперпозицією двох однофотонних станів гармонічних осциляторів, які відповідають двом ортогональним поляризованим коливанням електромагнітного поля.

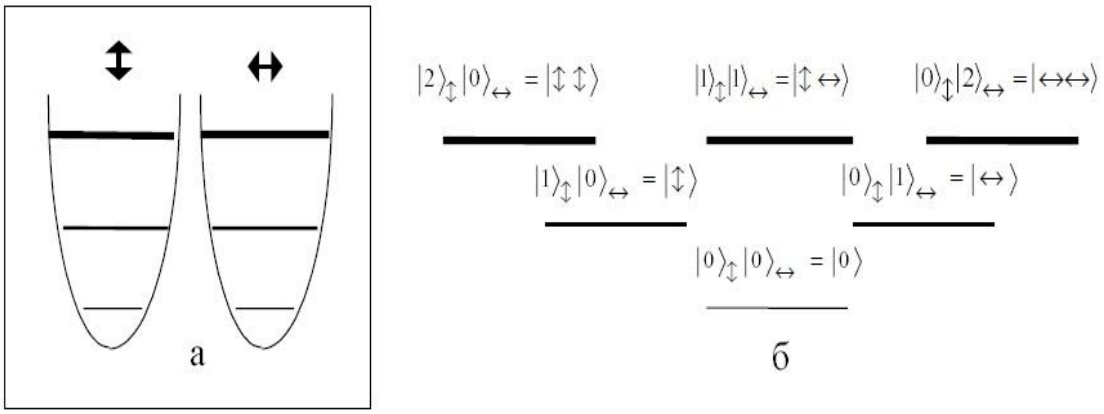

Рисунок 1.1 Світловий пучок з заданим хвильовим вектором

а) однофотонний стан пучка визначається суперпозицією двох породжених станів поляризованих фотонів;

б) двохфотонний стан пучка в загальному випадку є суперпозицією трьох енергетично породжених станів, два з яких - пара тотожно поляризованих фотонів, а одне – пара ортогонально поляризованих фотонів.

Коли мова йде про поляризаційні стани одного фотона – мають на увазі стан двохрівневої системи[3]:

$$\left|1_{\text{фотон}}\right\rangle = \mathrm{C}_{\leftrightarrow}\left|\leftrightarrow\right\rangle + C_{\updownarrow}|\updownarrow\rangle.$$

Під час проекційних вимірів детекторами одиночних фотонів, перед якими розміщені поляризатори, виділяючи горизонтальну або вертикальну поляризації, ймовірність відповідного вимірювання дорівнює $|C_{\leftrightarrow}|^2$ або $|C_{\updownarrow}|^2$. Якщо використовувати перед детекторами поляризатори, виділяючи поляризацію в 45° і 135°, то ймовірність їх спрацювання буде - $|C_{\leftrightarrow} + C_{\updownarrow}|^2$ або $|C_{\leftrightarrow} - C_{\updownarrow}|^2$ відповідно[3]. З цього випливає, що в діагональному базисі стан одного фотона можна еквівалентним шляхом представити в вигляді:

$$\left|1_{\text{фотон}}\right\rangle = \frac{(\mathrm{C}_{\leftrightarrow}+\mathrm{C}_{\updownarrow})}{\sqrt{2}}\left|\nearrow\right\rangle + \frac{(\mathrm{C}_{\leftrightarrow}-\mathrm{C}_{\updownarrow})}{\sqrt{2}}\ |\ \nwarrow\ |.$$

Поняття один фотон в розглянутому виникло як одне збудження об’єкта – світловий пучок з заданим хвильовим вектором, який складається з двох мод поля. Такий об’єкт є делокалізованим в просторі і не відповідає представленню про фотони, які локалізованих частинках, поширюваних у вільному середовищі зі швидкістю світла. Питання щодо локалізації фотона вирішується, беручи до уваги обставини в теоретичних міркуваннях про розповсюдження фотонів завжди присутнє поняття початкової (кінцевої) просторово-часовох точки, поява (зникнення) фотона. Локальність зникнення фотонів можна спостерігати за допомогою детекторів незалежно від локальності реєстрованого поля. Локальність появи фотона можна спостерігати, використовуючи джерела такого ж розміру. Однак, зважаючи на геометричний фактор, таке джерело буде обов’язково збуджувати ряд делокалізованих мод поля і тим самим створювати польовий об’єкт, який вже локалізований в просторі.

Для прикладу квантого об’єкта, який складається з багатьох мод поля демонструючого розповсюдження локалізовані однофотонні імпульси світла. Світловий імпульс з заданим направленням хвильового вектора –

багатоходовий об’єкт, створений з різночастотних мод поля. В залежності від розподілення амплітуд вхідних в нього мод, даний квантовий об’єкт може представляти собою різні по формі світлові імпульси, розповсюджувані в заданому направленні. До речі, чим ширше розподілення мод, тим більше локалізований відповідний імпульс світла.

Для визначення припустимо, що направлення розповсюдження імпульса співпадає з віссю z, то хвильові вектори плоских мод поля, що створюють імпульс, визначаються наступними декартовими компонентами[3]:

$$k_k = \left\{k_{kx} = 0, k_{ky} = 0, k_{kz} = \frac{2\pi}{L} m_z\right\} \tag{1.8}$$

Стан данного об’єкта в загальному випадку може бути таким складним, яким може бути сукупність станів сукупності гармонічних осциляторів. Простий приклад стану, відповідному однофотонному збудженню мод поля: $|\psi_{\text{однофотонний імпульс}}\rangle = \sum_v c_v a_v + |0\rangle$,

де $|0\rangle$ - вакуумні стани мод поля, c_v - комплексні амплітуди, квадрати модулів яких визначають ймовірність виявити фотон в v - моді.

1.2.2 Когерентні і інші стани оптичних полів

Когерентний стан було відкрито Шредінгером (Schrqdinger, 1926) під час розгляду гармонічного осцилятора і визначалось як стан з мінімальною невизначеністю. Когерентні стани є важливими для опису квантового опису оптичної когерентності.

Сам термін когерентності в квантовій оптиці ввів Глаубер (Glauber, 1963). Хвильова функція, яка використовується для класичного описання електромагнітного поля повинна мати мінімальну невизначеність для всіх

відрізків часу[2]. Такою властивістю володіє хвильова функція основного стану зміщеного простого гармонічного осцилятора, яка представляє собою хвильовий пакет, що виконує синусоїдальні коливання в потенціальному полі.

Відповідний вектор стану представляє собою когерентний стан і позначається $|a\rangle$. В квантовому стані гармонічного осцилятора хвильовий пакет не розбігається, а його центр рухається по класичній траєкторії. З класичної точки зору електромагнітне поле складається з хвиль із зазданими значеннями амплітуди і фази. Але при квантово-маханічному описі поля цей опис повністю відрізняється. В нашому випадку займають місце флуктуації як амплітуди, так і фази поля. Електромагнітне поле в стані $|n\rangle$, заданим числом частинок має визначену амплітуду, але повністю невизначену фазу, тоді як поле в когерентному стані має однакові величини невизначеності для двох змінних.

Вектор стану $|\psi(t)\rangle$ овної системи задовольняє рівняння Шредінгера: $\frac{d}{dt}|\psi(t)\rangle = -\frac{i}{\hbar}H|\psi(t)\rangle$, $|\psi(t)\rangle = \prod_{\mathbf{k}} \exp\left(\alpha_{\mathbf{k}} a_{\mathbf{k}}^{+} - \alpha_{\mathbf{k}}^{*} a_{\mathbf{k}}\right)|0\rangle_{\mathbf{k}}$, $|\psi(0)\rangle$ початкове значення є вакуумним $|0\rangle$. $\hat{\varepsilon}_{\mathbf{k}}$ одиничний ветор поляризації $E_к$ - напруженість електричного поля, $\hat{\varepsilon}_{\mathbf{k}}$ - частота.

$\alpha_{\mathbf{k}} = \frac{1}{\hbar \nu_{\mathbf{k}}} E_{\mathbf{k}} \int_0^{t'} dt' \int d\mathbf{r}\, \hat{\varepsilon}_{\mathbf{k}\mathbf{k}} \mathbf{J}_{\nu}(\mathbf{r},t) e^{i\nu_{\mathbf{k}}t' - i\mathbf{k}\cdot\mathbf{r}}$ стан поля $|\{\alpha_{\mathbf{k}}\}\rangle$ називається когерентним станом і позначається багатомодовий когерентний стан $|\{\alpha_{\mathbf{k}}\}\rangle = \prod_{\mathbf{k}} |\alpha_{\mathbf{k}}\rangle$, $|\alpha_{\mathbf{k}}\rangle = \exp\left(\alpha_{\mathbf{k}} a_{\mathbf{k}}^{+} - \alpha_{\mathbf{k}}^{*} a_{\mathbf{k}}\right)|0\rangle_{\mathbf{k}}$ когерентний стан поля, як власний стан оператора знищення a, з власним значенням α.

$a|\alpha\rangle = \alpha|\alpha\rangle$, стан $|\alpha\rangle$ можна виразити через стан з заданим числом частинок $|n\rangle$ наступним чином: $|\alpha\rangle = e^{-|\alpha|^2/2} \sum_{n=0}^{\infty} \frac{\alpha^n}{\sqrt{n!}} |n\rangle$, $|\alpha\rangle D(\alpha)|0\rangle$, $|\alpha\rangle = e^{\alpha a^{+}}|0\rangle e^{-|\alpha|^2/2}$, $D(\alpha) = e^{-|\alpha|^2/2} e^{\alpha a^{+}} e^{-\alpha^{*} a}$ [4]. Згідно з виразом когерентний стан отримуємо в

результаті використання оператора зміщення до вакуумного стану. Відповідно когерентний стан представляє собою зміщення основного стану гармонічного осцилятора. Для прикладу уявимо, що в момент часу t = 0 хвильова функція $\psi(q,t)$, $\Delta p\Delta q = (n+\frac{1}{2})\hbar$ має вигляд хвильового пакету з мінімальною невизначеністю, зміщеного в позитивну сторону направлення q на величину q0. $\psi(q,0) = (\frac{\nu}{\pi\hbar})^{1/4} \exp\left[-\frac{\nu}{2\hbar}(q-q_0)^2\right]$. Хвильова еволюція цього пакета заключається в тому, що в наступні моменти часу щільність ймовірності задається виразом[4] $|\psi(q,t)|^2 = (\frac{\nu}{\pi\hbar})^{1/2} \exp\left[-\frac{\nu}{\hbar}(q-q_0\cos\nu t)^2\right]$.

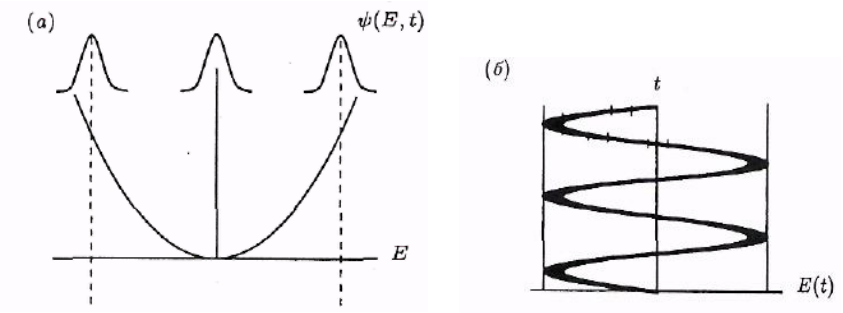

Рисунок 1.2 Хвильовий пакет з мінімальною невизначеністю в різні моменти часу в потенціальному полі гарнонічного осцилятора (а);відповідне електриче поле (б).

Властивості когерентних станів

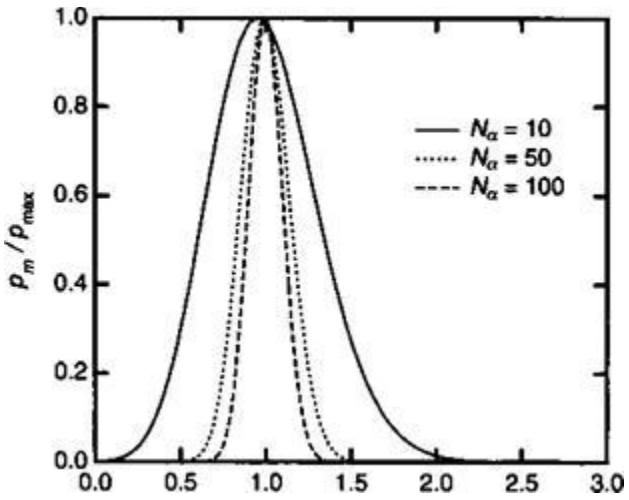

Рисунок 1.3. Розподілення фотонів

$p(n)$ - в когерентному стані, $p(n) = \langle n|\alpha\rangle\langle\alpha|n\rangle = \dfrac{|\alpha|^2 n e^{-\langle n\rangle}}{n!} = \dfrac{\langle n\rangle^n e^{-\langle n\rangle}}{n!}$.

Гамильтоніан осцилятора при наявності квадратичного потенціалу

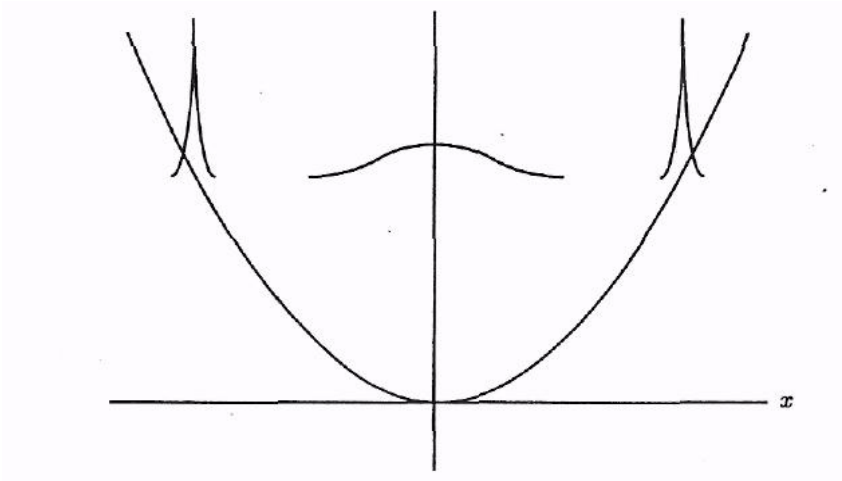

Рисунок 1.4. Еволюція стиснутого стану простого гармонічного осцилятора

Згідно з принципом невизначеності Гейзенберга зведення невизначеностей в визначенні середніх значень двох змінних A і B задається виразом $\mathbf{E}(t) = E\hat{\varepsilon}\left(ae^{-i\nu t} + a^+ e^{i\nu t}\right)$.

Кооперативний ефект – явище в багато частинній системі, зв'язане з когерентною взаємодією великої кількості частинок. Існують ефекти і явища, які залежать від стану і взаємодії групи атомів, при цьому групова і колективна поведінка атомної системи може бути відносно простою. Тоді досліджувати явище можливо шляхом сумування вкладів від індивідуальних атомів в загальне поле і гадати, що атоми діють майже незалежно один від одного. В інших випадках важливо враховувати вплив кожного атома на інші, оскільки це суттєво змінює поведінку кожного з них. Саме такі ефекти називають кооперативними.

Надтекучість і надпроводимість – це приклади кооперативних явищ, під час яких квантова когерентність проявляється в макроскопічних масштабах, а саме при участі електронно-фотонної взаємодії. Існують нерівноважні кооперативні явища, які виникають у відкритих системах, і їх існування зв'язано з дисипацією енергії. Випромінювання лазера – приклад нерівномірного кооперативного явища, коли при достатньо високому ступені нерівномірності (потужність накачки) безструктурний стан системи стає нестійким до малих флуктуацій, шо супроводжується генерацією випромінювання.

1.3 Квантова інформатика

Квантова інформатика – наука нових ресурсів, які тільки відкриваються за допомогою квантових об'єктів для вирішення задач, в свою чергу відносяться до області «інформатика» - комунікації, захист, розрахунок. В свою чергу квантова інформатика ділиться на декілька підрозділів: квантова комунікація, квантова криптографія, квантові розрахунки.

В квантовій інформатиці є сенс замінити класичні об'єкти на квантові, але при цьому доведеться зіштовхнутись з рядом проблем. Наприклад, в

класичному випадку не виникає ускладнень з нумерацією об'єктів для вибору: червона куля – з номером 1, оранжева -2, жовта -3 і так далі. Якшо припустити, що так само вчинимо з квантовими об'єктами в двохвимірному гільбертовому просторі, використовуючи, наприклад таблицю нумерації цих об'єктів:

Таблиця 1.1 Номерація об'єктів

Номер объекта (i)	1	2	3	4
Состояние $\|\psi_i\rangle$	$\|0\rangle$	$\|+\rangle = \frac{\|0\rangle+\|1\rangle}{\sqrt{2}}$	$\|1\rangle$	$\|-\rangle = \frac{\|0\rangle+\|1\rangle}{\sqrt{2}}$

Аліса створює ці об'єкти зі свого боку і передає їх Бобу. Боб отримує ці квантові об'єкти і намагається прочитати їх номер за допомогою вимірів. Саме на цьому етапі виникає проблема. Вибираючи в якості виміру будь-який з типів вимірів, він розуміє що не може розрізнити всі неортогональні стани. Так вибираючи проекційний тип виміру,$P_{|0\rangle} = |0\rangle\langle 0|$, $P_{|1\rangle} = |1\rangle\langle 1|$, Боб буде отримувати наступні результати з ймовірністю[3]:

Таблиця 1.2 Номерація об'єктів

Номер объекта (i)	1	2		3	4	
Результат измерения $P_{\|k\rangle}$	$\|0\rangle$	$\|0\rangle$	$\|1\rangle$	$\|1\rangle$	$\|0\rangle$	$\|1\rangle$
Вероятность $\langle\psi_i\| P_{\|k\rangle} \|\psi_i\rangle$	1	1/2	1/2	1	1/2	1/2

Тобто достовірність відправлених станів буду лише для першого і третього об'єкта. Вибір проекційних операторів виміру в вигляді $P_{|+\rangle} = |+\rangle\langle +|$, $P_{|-\rangle} = |-\rangle\langle -|$ дозволить відрізнити другий і четвертий об'єкти, в той час як перший і третій буде неможливо відрізнити. Цим прикладом показано, що незважаючи на нескінченне число станів дворівневої системи, допустимих для розпізванання станів тільки два.

Квантова система з двома рівнями може переносити 1 біт інформації. Називається така система кубіт (квантовий біт). Зазвичай «дворівневими» називають квантові системи з двома рівнями енергії. В даному випадку система характеризується двома станами

Неможливість розрізнити неортогональні стани квантових систем показує, що квантові стани містять в собі засекречену інформацію, яку неможливо проявити під час виміру, з цього випливає, що вона може бути використана для криптографії і обчислень.

Неможливість розрізнити неортогональні стани призводить до принципового висновку. Якшо Боб отримав неортогональні повідомлення і міг розрізнити їх, то він би отримав можливість зробити безліч копій цих неортогональних станів. Неможливість зробити копію невідомого квантового стану має назву теореми неможливості клонування невідомого квантового стану [3]. Загалом цю теорему виводять як наслідок лінійності квантової механіки.

Відсутність можливості клонування невідомих станів і еквівалентна неможливість ідеального розрізнення неортогональних станів не завжди негативні і їх можна використовувати.

З теореми неможливості клонування можна отримати оцінку для величини доступної квантової інформації в комунікаційній схемі[3]. Наприклад, нехай Аліса відправляє Бобу послідовність квантових систем в неортогональних станах з ймовірністю ρ та $1-\rho$. Якщо Боб, отримуючи неортогональні стани, може їх клонувати, то створюючи багаточасткові стани, він міг би їх розрізняти з більшою точністю, внаслідок того, що багаточасткові стани стають майже ортогональними. Відповідно, в цьому випадку він отримав можливість розрізняти неортогональні стани у відправленій послідовності. Величина доступної інформації дорівнювала б класичній. Хоча для довільних схем загальний спосіб підрахунку доступної квантової інформації невідомий,

існує ряд граничних оцінок для такої величини. Однією з важливих є квантова ентропійна границя.

1.3.1. Переплутані квантові стани

Використання світлових сигналів викликає інтерес при вирішенні проблеми передачі квантової інформації. Визначення типу світлових полів володіє рядом властивостей, які безпосередньо використовуються в квантових комунікаційних протоколах, таких як квантова телепортація та квантове розподілення ключа. Ці поля розглядаються як квантові системи, спроба їх виміру призводить до збудження стану. Взагалі під некласичним розуміється світло, властивості якого неможливо описати класичним чином і виділити його відмінні сторони. Всі ці проблеми разом складають предмет квантової оптики.

З точки зору експеримента, властивості світлових полів можливо дослідити, аналізуючи властивості фотоку, які їм породжуються. При цьому аналогічно аналізувати їх середній потік і його флукрутацію. Відомо, що середній потік пропорційний інтенсивності світла, падаючого на фотодетектор. Флуктуацію фотоку можливо пояснити випадковістю породження фотоелектронів в процесі детектування, тому доволі довгий час їм не придавали особливого значення. Такі флуктуації називають пуасснонівськими або дробовим шумом. Існує співвідношення і критерії, які встановлюють зв'язок між характеристиками, які ми спостерігаємо, фоток і статистичні властивості світла.

Переплутування – це поняття, яке відноситься до двох чи більше адресуємих систем. Формально в квантовій механіці дві системи A і B можна розглядати як одну складову систему AB з гільбертовим простором, що представляє собою пряме відтворення гільбертових просторових систем A і B.

В загальному просторі відтворення вектора для системи А і вектор для системи В. такий вектор називається переплутаним станом систем А і В.

Переплутані стани створюються в результаті взаємодії двох систем А і В, але розглядаються і використовуються вже після закінчення взаємодії. Протягом 30 років переплутані стани успішно створюються в лабораторіях по всьому світу. Об'єктами для створення переплутаних станів служать різні частинки з різними степенями свободи, використовувані для кодування станів: фотони в поляризаційних, фазових, просторових і інших станах, електронні і ядерні спіни в різних структурах і матеріалах, квантові стани надпровідних комірках та інші системи.

Найбільш широко використовуваним видом переплутування є поляризаційне переплутування – створення поляризаційного стану двох фотонів, які породжуються в нелінійному кристалі під дією оптичної накачки в процесі спонтанного параметричного розпаду. Фотони породжуються в синглетному стані $|\psi\rangle$, де $|0\rangle$ відповідає горизонтальній поляризації, а $|1\rangle$ – вертикальній[5].

Переплутані стани є необхідним квантовим ресурсом для реалізації протоколів квантової телепортації, надщільного квантового кодування, а також деяких протоколів квантової криптографії, наприклад, протокол Екерта. Переплутані стани лежать в основі квантових підрахунків і комп'ютерів. Є невід'ємною частиною у вивченні квантової теорії, через те, що вони призводять до ефектів, які не можна пояснити з точки зору локального реалізму в теорії ймовірності.

1.4. Основи криптографії

Квантова криптографія – розділ квантової інформатики, що вивчає методи захисту інформації шляхом використання квантових носіїв (фотонів).

Можливість реалізації такого захисту реалізується теоремою про неможливість клонування невідомого стану квантового об’єкта [6].

Історично під криптографією розумілось мистецтво тайнопису, тобто перетворення осмисленого тексту в незрозумілий шифр з метою його захисту. Шифрування тексту може використовуватись для зберігання інформації, так і для секретної відправки кінцевому користувачу, який в свою чергу володіє алгоритмом дешифровки. Роблячи висновок, традиційна криптографія забезпечувала конфіденційність інформації навіть за умови доступу до неї сторонніх осіб. В 20 столітті криптографія перетворилась в окрему наукову дисципліну зі своїми науковими журналами, книгами та міжнародними конференціями [3]. В нащ час інформаційне суспільство в значній мірі зв’язано з цифровою технікою, а разом з цим поняття криптографія розширилось і зв’язується з комплексними методами захисту інформації, які, окрім конфіденційності, забезпечують її цілісність і проведення процедури аутентифікації. Цілісність – це неможливість її непомітно змінити або підмінити, аутентифікація – складається з встановлення особистості сторін, які вступають в обмін інформацією. Таким чином, захист інформації полягає в охороні законних користувачів, які обмінюються інформацією, від дій зловмисника, який намагається прочитати інформацію або змінити її. В поняття захисту вкладено також захист законних користувачів один від одного, що є важливим в елетронній торгівлі.

Звісно, не кожний захист інформації має відношення до криптографії. Для забезпечення конфіденційності документи зберігають в сейфах, цілісність забезпечується підписами та печатками, а аутентифікація – за допомогою особистих даних. Криптографія відрізняється від інших способів специфічними методами. На початку 90-х років криптографію асоціювали з наукою, яка вивчала математичні методи захисту інформації. Після появи квантової криптографії це поняття стало «малим».

Під час використання простого методу шифрування – безпека буде втрачена, якшо зловмиснику стане відомий алгоритм шифрування. Історія показує, що при забезпеченні зв'язку між великими організаціями в секреті алгоритм шифрування тримати неможливо і періодично міняти – нерентабельно. Через це науковці прибігають до іншого прийому. У функції шифрування і дешифрування вводиться додаткова змінна – криптографічний ключ $C = f_e(T)$, $T = g_d(C)$, де e – ключ шифрування, а d - ключ дешифрування[3]. Алгоритми шифрування повинні задовольняти рівність $g_d(f_e(x)) = x$ для будь-якого x з безлічі значень початкового тексту для того, щоб дешифрований текст співпадав з початковим. Таким чином для забезпечення безпеки необхідно зберігати в секреті і періодично змінювати тільки декілька ключів, а самі алгоритми можна оприлюднювати. Інколи алгоритми спеціально публікують для знаходження критичних для безпеки недоліків.

Висновок з розділу 1

Квантова криптографія зарекомендувала себе як надійна система, яка не піддається поки що відомим методам дешифрування сторонніми особами. Може використовуватись в банківській та воєнній сфері. Завдяки відмінності квантової теорії від класичної фізики стає можливо забезпечити повну безпеку передачі інформації по лінії зв'язку.

Сторонні особи, які будуть намагатись прослухати інформацію, можуть витягнути частину інформації, яка передається, але це не дасть ніякого результату, тому що сторонній користувач обов'язково змінить стан передаваємих частинок.

РОЗДІЛ 2. ПРОТОКОЛИ КВАНТОВОГО РОЗПОДІЛЕННЯ КЛЮЧА

2.1. Протокол BB84

BB84 протокол, розроблений Чарльзом Беннетом и Жильем Брассаром, був запропонований в 1984 році і є першим протоколом квантового розподілення ключа [7]. Протокол заснований на принципах квантової механіки, що робить його абсолютно безпечним при відсутності шуму в квантовому каналі зв'язку, і використовуючи частинки, що передаються і не допускають їх клонування. Виконання цих умов називається ідеальними умовами для квантоного розподілення ключа

Відсутність шуму дає змогу визначити, що квантові стани частинок не змінюються при розповсюдженні по квантових каналах зв'язку. Згадуючи класичну теорію інформації, початково вважається, що повідомлення завжди можна перехопити і прослухати, а також скопіювати його без зміни його змісту. Але якщо інформація зашифрована в неортогональних квантових станах, то стани фотонів з поляризацією 0°, 45°, 90°, 135°, то зловмиснику прочитати або скопіювати її повністю принципіально неможливо. Зловмисник не зможе отримати з повідомлення навіть частину інформації, не змінивши її випадковим чином, який з великою вірогідністю буде помічено легітимним користувачем каналу зв'язку.

Спочатку протокол BB84 був сформований для одиночних фотонів, хоча його можно перевести на інші реалізації кубітів. Для кодування інформації в протоколі використовується чотири стани поляризації, які створюють два базові неортогональні один для одного базиси $\leftrightarrow$ і $\updownarrow$, а також діагональний $|\nearrow\rangle = (|\leftrightarrow\rangle + |\updownarrow\rangle)/\sqrt{2}, |\nwarrow\rangle = (|\leftrightarrow\rangle - |\updownarrow\rangle)/\sqrt{2}.$

Суть полягає в тому, що один з користувачів, для прикладу, Аліса вибирає випадковим чином послідовність бітів і послідовність базисів, після

цього посилає іншому користувачеві – Бобу – послідовність фотонів, кожен з яких кодує один біт з вибраної послідовності в базисі, відповідаючий порядковому номеру цього біта, стани ↔ і ⤢ кодують 0, а ↕ і ⤡ в 1.

Під час отримання фотонів Боб випадковим чином для кожного фотона незалежно від Аліси вибирає базис для виміру і аналогічним чином для кожного фотону інтерпретує результат своїх вимірів як двійковий 0 або 1. Згідно до законів квантової механіки, після виміру діагонального фотона в прямокутному базисі його поляризація перетворюється в горизонтальну або вертикальну, зважаючи на результати виміру або навпаки, при цьому результат виміру буде випадковим. Таким чином Боб отримає результати, які співвпадають із станом відправлених фотонів в половині випадків, тобто коли він правильно вгадав базис.

Наступним кроком протоколу виконується за допомогою відкритого каналу зв’язку, Аліса і Боб можуть відкрито повідомляти один одному класичну інформацію. Припустимо, що класична інформація не змінюється при розповсюдженні по відкритому каналу. Це означає, що можливе пасивне підслуховування, тобто зловмисник може читати повідомлення двох сторін, але не може змінювати і відправляти повідомлення за них.

Таблиця 2.1 Реалізація протоколу BB84 за відсутності шуму

1. Случайные биты (Алиса)	0	1	1	0	1	1	0	0
2. Случайные базисы (Алиса)	⊗	⊗	⊗	⊕	⊕	⊗	⊗	⊕
3. Поляризация фотонов, передаваемых по *квантовому каналу*	↗	↘	↘	↔	↕	↘	↗	↔
4. Случайные базисы приема (Боб)	⊕	⊕	⊗	⊗	⊕	⊕	⊕	⊕
5. Полученные Бобом биты	0	0	1	1	1	0	0	0
6. Боб сообщает Алисе базисы измерений (*классич. канал*)	⊕	⊕	⊗	⊗	⊕	⊕	⊕	⊕
7. Алиса сообщает, какие из них верны (*классич. канал*)			✓		✓			✓
8. Полученные общие биты (просеянный ключ)			1		1			0
9. Боб открывает часть битов					1			
10. Алиса подтверждает их					✓			
11. Полученный в итоге ключ (просеянный ключ после оценки ошибки, вызванной возможным подслушиванием)			1					0

В першу чергу Аліса і Боб визначають шляхом відкритого обміну повідомленнями, які фотони були успішно отримані, які з них були змінені Бобом в правильному базисі. Потім Аліса і Боб будуть мати однакові значення бітів, зашифрованих в цих фотонах, не дивлячись на те, що ця інформація ніколи не обговорювалась по відкритому каналу. Кожен з фотонів несе один біт випадкової інформації, яка відома Алісі та Бобу і більше нікому. Інформація про фотони у виміряних в неправильному базисі відкидаються, в результаті чого Аліса і Боб отримують просіяний ключ, який при відсутності прослуховування повинен бути однаковим в обох сторін.

Не пропускаючи факт того, що також можливе прослуховування, зловмисником буде виступати Ева, розглянемо приклад. Через випадковий вибір прямокутного або діагонального базиса вимірювання фотонів при обміні квантовими повідомленнями Ева змінює повідомлення таким чином, що Аліса і Боб знаходять зміни в бітах просіяного ключа, які за умови відсутності прослуховування повинні співпадати. Жоден вимір переданого фотона Евою, яка дізнається про початковий базис в фотоні лише після того, як зробить його вимір, не може дати більше ½ інформації про біт, кодуємий цим фотоном, будь-які зміни даючі b біт інформації, повинно давати неузгодженість з ймовірністю b/2, якщо виміряний фотон або його заміна в подальшому буде виміряна Бобом в початковому базисі. Такий спосіб підслуховування, коли Ева вимірює і передає далі всі перехвалені фотони в прямокутному базисі, дізнаючись в такому випадку правильну поляризацію половини фотонів і вносячи зміни в четверту частину фотонів, які будуть потім виміряні в початковому базисі.

Виходячи з вище сказаного, Аліса і Боб можуть перевірити наявності факту підслуховування, відкрито порівнюючи частину бітів, про які у них повинна бути однакова інформація, хоча це зробить біти непридатними для використання в секретному ключі. Положення бітів під час цього порівняння повинні бути випадковою множиною правильно виміряних бітів так, щоб підслуховування більш ніж декількох бітів не могло уникнути виявлення Еви. Якшо всі біти порівнювальні біти співпадають, Аліса і Боб роблять висновок, що підслуховування немає, і біти, які залишились, можна безпечно передавати в якості секретного ключа для наступного шифрування даних і передачі по відкритому каналу.

Коли ключ вже використаний, Аліса і Боб знову повторюють всю процедуру і отримують наступний секретний ключ.

2.2. Протокол B92

Протокол B92 був запропонований в 1992[8] році Чарльзом Беннетом, звідси і назва протоколу. Протокол був заснований на принципах невизначеності на відміну під протоколу E91. Носіями інформації дворівневої системи – кубіти. Особливість протоколу – використання двох неортогональних квантових станів.

Для генерації криптографічного ключа по протоколу B92 використовується та ж сама схема, що і для протоколу BB84, але замість чотирьох станів використовують тільки два неортогональні стани.

При зміні квантого біта на стороні Боба проводитmся випадковий вибір одного з двох базисів. Якщо при виборі прямолінійного базиса $\{|\leftrightarrow\rangle, |\updownarrow\rangle\}$ результатом виміру виявилось $|\leftrightarrow\rangle$, Боб знає, що відправлявся стан $|\nearrow\rangle$ і записує його в свою послідовність 1. Аналогічно, якщо при виборі косокутного базиса $\{|\nearrow\rangle, |\nwarrow\rangle\}$ результатом виміру виявилось $|\nwarrow\rangle$, відправлявся стан $|\updownarrow\rangle$ і записує його як 0. Всі інші результати вважають нерезультативними і не враховують. В протоколі відсутня процедура погодження базисів, замість неї Боб повідомляє Алісі по відкритому каналу номер результативних вимірів, в подальшому по результатах генерується просіяний ключ. Ева, знаючи номер результативних вимірів, не в стані правильно визначити значення переданого біта через стан його кодування – неортогональний, тобто неможливо відрізнити.

На жаль, протокол B92 не зміг стати конкурентом для протоколу BB84 через свої недоліки. Існує ряд труднощів в реалізації протоколу:

1) Недосконалі джерела одиночних фотонів, а саме швидкість генерації;
2) Недосконалість детекторів одиночних фотонів – спрацювання датчика не тільки на фотони, але і на інші частинки;

3) Сучасні волоконно-оптичні лінії не гарантують досягання фотоном кінцевої точки;

4) Ціна встановлення такої системи приблизно оцінюється в сотні євро, але повсякденне використання такої системи не передбачається.

Незважаючи на недоліки перед іншими протоколами, протоколом B92 зручніше користуватись через простоту його реалізації. У зв'язку з цим були проведені експерименти по його реалізації. Вчені з Бразилії в своїй статті описали установку, за допомогою якої реалізували протокол. У висновку вони звернули увагу на проблеми, які виникли в процесі установки, і описали методи їх усунення. Так само група вчених з Китаю зібрали установку довжиною 2.2 метра і поставили експеримент по передачі інформації за допомогою протоколу B92 і відмітили, що для передачі фотона на великі відстані потрібно замінити протокол.

2.3. Протокол Екерта

Квантовий криптографічний протокол заснований на експерименті Енштейна-Подольского-Розена і узагальнений в теоремі Белла. Був запропонований польським фізиком Артуром Екертом в 1991 році[9]. Протокол заснований на властивостях заплутаних станів квантових частинок. Для цього Екерт використовував пару частинок – ЕПР пару.

В протоколі пропонується використовувати пару фотонів породжених в асиметричних поляризаційних станах. Перехоплення одного з пари фотонів не приносить Еві ніякого результату, але для Аліси і Боба є сигналом того, що канал прослуховується.

Ефект ЕПР виникає, коли сферично симетричний атом випромінює два фотона в протилежних направленнях в сторону спостерігачів. Фотони

випромінюються з невизначеною поляризацією, але в силу симетрії їх поляризації завжи протилежні. Важливим фактором цього ефекту є те, що поляризація фотонів стає відомою тільки після вимірювання. На основі ЕПР Екерт запропонував протокол, який гарантує безпеку відправлення і зберігання ключа. Відправник генерує деяку кількість ЕПР фотонних пар. Один фотон з кожної пари він залишає собі, другий – відправляє. При цьому якщо ефективність реєстрації близька до одиниці, при отриманні відправником значення поляризації 1, його співбесідник зареєструє значення 0 або навпаки. Таким чином, співрозмовники кожного разу, коли потрібно, можуть отримати однакові псевдовипадкові кодові послідовності.

2.4. Шум і перехват інформації в каналі

В реальній ситуації в квантовому каналі зв’язку завжди є наявність шуму. Під шумом розуміють викривлення класичної інформації, закодованої в квантовому носії під час розповсюдження по квантовому каналі. Джерела шуму можуть мати різну фізичну природу. Наявність шуму в каналі призводить до того, що після виконання протоколу квантового розподілення ключів (КРК) випадкові послідовності, отримані Алісою та Бобом, будуть різнитись між собою [3]. Зрозуміло, що за наявності такого шуму, Ева може цим скористатись. Наприклад, Ева може замінити частину квантового каналу на менш шумний і провести свої виміри так, щоб загальний рівень шуму, контрольований Алісою і Бобом, не буде перевищено. В такому випадку Аліса і Боб не будуть знати, що їх прослуховують. Щоб забезпечити якомога мешний вплив шуму потрібно зробити аналіз:

1) Оцінка рівня шуму в просіяних ключах Аліси і Боба;

2) Способи, які може використати Ева для перехоплення повідомлення;

3) Теоретична оцінка величини інформації, якою буде володіти Ева в результаті перехоплення;

4) Процедури, що дозволяють оброблювати ключі Аліси і Боба таким чином, щоб вони не містили інформації, яку Ева перехопила – вторинна обробка ключа (корекція помилок).

Після етапу просіювання сирих ключів в схемі КРК, Аліса і Боб мають дві двійкові послідовності – просіяні ключі, які не співпадають в деяких позиціях через шум. Важливо визначити рівень шуму в отриманих просіяних ключах.

Позначимо довжину просіяного ключа N_s, а відношення неспівпадаючих бітів в просіяних ключах до довжини цього ключа Q. Цю величину Аліса і Боб можуть оцінити, виконуючи протокол визначення рівня шуму:

1) Аліса випадково вибирає послідовність номерів, менших N_s;

2) Аліса відправляє Бобу по класичному каналу цю послідовність разом зі значеннями бітів, маючих відповідні номери;

3) Боб порівнює значення бітів Аліси зі значеннями своїх бітів, маючих ті ж номери, вираховуючи кількість бітів, які не співпадають;

4) Аліса і Боб виключають скомпрометовані біти з послідовностей, отримуючи просіяні послідовності.

На стадії лабораторного тестування лінії КРК встановлюється робоче Q_0 і максимальне $Q_m > Q_0$ значення рівня шуму в квантовому каналі, відповідні довжині лінії КРК. Насправді лінії КРК на одиночних фотонах Q_0 і Q_m складають декілька відсотків при довжині лінії до 50 кілометрів. Перевищення шумом каналу максимального рівня Q_m розцінюється як перехоплення. В цьому випадку користувачі лінії КРК відмовляються від генерації ключа і займаються пошуком Еви в квантовому каналі.

2.4.1. Маскування перехоплення під шум. Види перехоплення

Задача перехоплювача Еви – отримати максимум інформації про ключ і не бути поміченою. Як відомо, будь-яка спроба перехоплення інформації призводить до збільшення рівня шуму в квантовому каналі. Насамперед Ева може використовувати різницю між робочим рівнем шуму Q_0 і максимальним рівнем Q_m. Якщо шум не перевищує максимальний рівень до робочого – перехоплення буде непомітним. Це найбільш реальний спосіб перехоплення через те, що вона потребує підключення до квантового каналу лише в одній точці. Під час аналізу захищеності лінії КРК роблять більш вагомі припущення щодо Еви. Передбачається, що Ева може володіти будь-якою технологією. В результаті у Еви вже є план перехоплення: Ева робить заміну шумного квантового каналу на ідеальний і перехоплює інформацію в цьому каналі, вносячи шум не більше Q_m. В такому випадку весь шум квантового каналу буде результатом перехоплення, що забезпечує Еві максимальну інформацію про кінцевий ключ.

Всі атаки на квантовий канал розділяються на два: основний клас – пов’язані з квантовою природою носія інформації, специфічні – недосконалість апаратури. Атаки другого класу пов’язані з фізичною реалізацією криптографічної лінії [3].

Для перехоплення Ева повинна зробити квантові вимірювання. Квантове вимірювання може бути прямим – коли квантова система безпосередньо взаємодіє з вимірювальним пристроєм, або непрямим – коли квантова система взаємодіє з пробною системою, яка надалі піддається прямому виміру.

Відповідно по типу виміру атаки Еви розділяються на: прямі і непрямі. Також атаки Еви діляться відповідно до об’єкта виміру. Об’єктом виміру одного вимірювального процесу може бути окремий носій інформації в квантовому каналі. В цьому випадку атака – індивідуальна. У випадку, коли

вимірюванню піддаються декілька носіїв – спільна атака. Когерентна атака є більш технічно складною, але інформативною.

У випадку непрямої атаки існує такий варіант, коли кожен носій вступає у взаємодію з окремою пробною системою, а подальші виміри йдуть над блоками з декількох пробних систем, такий тип атаки називається колективним.

При будь-якому методі перехоплення Ева в результаті отримує деяку кількість числової послідовності N_E. Без обмеження спільності можна рахувати, що її довжина співпадає з довжиною сирого ключа Аліси і Боба N_R - послідовність перехопленого сирого ключа. На стадії просіювання Еві доступна вся інформація, якою обмінюються Аліса і Боб по класичному каналу. Ева виключає з сирого ключа ті ж самі біти, що Аліса і Боб. Після чого Ева отримує перехоплений просіяний ключ, який несе часткову інформацію про просіяний ключ.

Аліса і Боб для того, щоб зробити непридатною інформацію про просіяний ключ Еви, використовують відомі криптографічні процедури корекції помилок і посилення секретності. Знаючи рівень шуму в просіяному ключі, Аліса і Боб проводять процедуру корекцій помилок і отримують ідентичні виправлені ключі (ВК). Ева, спостерігаючи за відкритим каналом, по якому Аліса і Боб узгоджують виправлення помилок, такой робить корекції в перехопленому ключі і отримує перехоплений виправлений ключ (ПВК).

Непряме індивідуальне перехоплення. На даний момент непрямі виміри окремих фотонів робили тільки з дуже малою вірогідністю успіху. Проте непрямі виміри більш інформативні, ніж прямі при тому ж самому рівні внесеного шуму, тому методи захисту криптографічного ключа повинні включати таку можливість перехоплення. При непрямому вимірі кубика S, який знаходиться у відомому стані, Ева проводить його у взаємодію з пробною системою P, яка має чотири квантові рівня. Пробна система початково підготовлена в чистому вигляді. Взаємодія описується унітарним

перетворенням U в загальному просторі станів S і P. Параметри перетворення вибирають таким чином, щоб отримати максимум інформацію отриману при виміряному кубіті. Після взаємодії кубіт і пробна система переходять в стан пробної системи – тобто стан пробної системи корельовано із станом кубіта. Після взаємодії кубіт продовжує рух по квантому каналу, а пробна система зберігається Евою до стадії погодження базисів. Така затримка в вимірі P дає Еві можливість провести виміри з розрахунком відомостей, в якому базисі знаходився кубіт S до взаємодії. Квантова пам'ять – здатність зберігати квантову інформацію протягом декількох мілісекуд. Аналіз оптимальних параметрів взаємодії і оптимального виміру пробної системи пропонує наступний вираз для інформації Еви про виправлені ключі[3]:

$$I_E(Q) = \log_2(2 - (3 - \frac{2}{1-Q})^2). \quad . \quad (2.1)$$

На будь-якому рівні шуму інформація Еви при оптимальній непрямій атаці вище або дорівнює її інформації при прямій атаці проміжного базиса. В робочому рівні щуму близько 5%, це перевищення складає більше двох разів, тобто інформація Еви про ВК приблизно дорівнює 20%.

Колективне перехоплення. Під час атаки на BB84 Ева використовує взаємодію кожного кубіта, який протікає в квантовому каналі з окремою пробною системою. Вона зберігає всі пробні системи в квантовій памяті до стадії корекції помилок. Після цього Ева вимірює всі пробні системи, які залишились для отримання інформації про виправлений ключ. Колективний вимір всіх пробних систем забезпечить Еві потенційною багато інформації, якою Аліса і Боб обмінюються на стадії корекції помилок. Але параметри колективного виміру не були опубліковані. Обчислення верхньої границі цієї інформації не має інтересу через те, що обмежена зверху максимальноє інформацією, доступній Еві при когерентному перехопленні.

Когерентне перехоплення. Ева розглядає послідовність декількох кубітів, які розповсюджуються по квантовому каналі як одну квантову систему і намагається отримати максимальну інформацію про її стан.

Під час прямого когерентного перехоплення Ева проводить пряме колективне вимірювання декільков кубітів. Можливості перехоплення обмежені кількістю одночасно знаходженості в квантовому каналі носія. Середня відстань між послідовними носіями значення сирого біта перевищує довжину криптографічної лінії, що робить такий вид перехвату неможливим. Поки що відсутні відомості про прямий когерентний перехват.

Під час непрямого перехоплення Ева має одну пробну систему з великою кількістю квантових рівнів. Пробна система по черзі взаємодіє зі всіма кубітами, які поширюються в квантовому каналі. Стан квантової системи зберігається в квантовій пам'яті до моменту закінчення стадії виправлення помилок. Далі Ева проводить виміри пробної системи з урахуванням всієї інформації, перехопленої в класичному каналі і отримує ПВК. Наразі вважається, що непряма когерентна атака найбільш ефективна, тому що забезпечує Еві максимум інформації про ВК. Але жоден протокол ефективної атаки не був опублікований. Всі атаки призводять до висновку їх ідентичності індивідуальним атакам в розумінні отриманої інформації.

Висновок з розділу 2

Протоколи КРК мають ряд переваг перед класичними протолоками передачі інформаці.Можливість виявлення атаки пасивного перехоплення – атака Еви вносить значну кількість помилок, ніж їх виникає в квантовому каналі в результаті природного шуму. Теоретично-інформаційна стійкість ключів розподілення, ключі розподіленя за допомогою квантових протоколів з теоретико-інформаційною стійкістю в подальшому використовуються для

шифрування з використанням відомих класичних симетричних алгоритмів, внасідок чого загальний рівень крипостійкості підвищується.

Також існують недоліки таких протоколів. Для КРК необхідна попередня аутентифікація користувачів. Довжина ключа обмежена через те, що ще не розроблені квантові повторювачі. Залежно від збільшення довжини ключа зменшується швидкість передачі. Проблема реєстрації фотонів на детекторах внаслідок дії темнового шуму.

РОЗДІЛ 3. Квантове розподілення ключа одиночними фотонами

3.1 Джерела одиночних фотонів

Основним методом КРК складає передача ключа за допомогою одиночних фотонів, поляризація яких задається значенням бітів ключа. Секретність КРК забезпечується однофотонним квантовим носієм інформації, оскільки будь-яка зміна стану призводить до зміни поляризації, що робить неможливим клонування носія інформації після перехоплення з ціллю подальшої передачі. Якщо КРК проходило за допомогою багатофотонних імпульсів, кожен з яких складається з фотонів з однаковими значеннями бітів ключа, то виміри фотонів над одним фотоном змінить його стан. Але невикористані фотони під час вимірювання дозволяють визначити значення біта, який передається. Звідси випливає один з ключових елементів ряду квантової криптографічної системи, виявляється джерело одиночних фотонів (ДОФ) [3].

В ідеальному стані ДОФ повинно генерувати ряд фотонів, випускаючи з достовірністю в необхідні моменти тільки один фотон, при цьому фотони повинні бути невідмінні. Важливим для практичного застосування характеристиками ДОФ є довжина хвилі $\lambda_{доф}$ генерувальних фотонів і частота їх повторення $\omega_{доф}$, оптимальні величини яких визначається значною мірою ступеня характеристик других складових частин криптографічної системи. Вибір $\lambda_{доф}$ системи — компроміс між вимогами, які накладаються середовище розповсюдження фотонів і можливості їх детектування. З одного боку довжина хвилі генерувальних одиночних фотонів повинна бути такою, щоб їх поглинання при передачі від джерела до детектора було мінімальним, з іншого боку — для вибраної довжини хвилі повинні бути чутливі детектори. У випадку передачі ключа у відкритому просторі (повітрі) довжина хвилі $\lambda_{доф}$ повинна

потрапляти у вікна прозорості атмосфери. В більшості випадків вибираються вікна 750-800 нм або 850-900 нм, для яких є ефективні мало-шумні лавинні кремнієві детектори одиночних фотонів, які працюють в діапазоні 600-900 нм. З використання при передачі ключа існуючих телекомунікаційних мереж на стандартному одномодовому волокні найбільш прийнятним є довжини λдоф $\approx$1,31 мкм і λдоф $\approx$1,55 мкм, забезпечіючі надалі мале поглинання можливості передачі ключа на відстані порядку 100-150 км. Для таких хвиль використовують лавинні детектори на InGsAs-InP, але, на жаль, їх характеристики не завжди для практичних задач квантової криптографії. При менших відстанях у волоконних системах КРК можна використовувати ДОФ, генеруючі фотони на довжинах хвиль близько 840 нм, оскільки на суттєво великі поглинання у волокні для реєстрації можна використовувати кремнієві лавинні детектори. Так само для забезпечення великої швидкості передачі ключа частота повторення ωдоф $= 2\pi$/Тдоф, де Тдоф — час між одиночними фотонами, повинна бути наскільки можливо великою, але залишатись обмеженою зверху величиною мертвого часу детектора, який використовується для реєстрації одиночних фотонів [3]. Додатковими вимогами до ДОФ — тривала стабільна робота при умові кімнатних температур, простота маніпулювання стану генеруючих фотонів, їх збір і передача у визначеному просторовому направленні.

На сьогодення в експериментальній і практичній квантовій криптографії в якості ДОФ використовують різноманітні джерела світла, які частково задовольняють потреби. Джерела поділяють на три основні групи:

1) ослаблених лазерних імпульсів;

2) генерації корельованих пар фотонів в процесі параметричного розпаду в кристалах з квадратичною (4 степеню) нелінійністю;

3) одиночні квантові системи (атоми, молекули, іони).

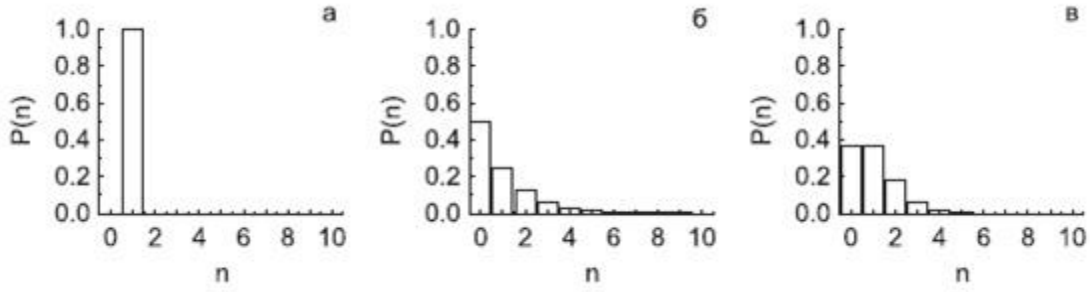

Рисунок 3.1 розподілення P(n), якщо n=1: а — для ідеального ДОФ, б — теплового джерела, в — лазерного джерела.

В лабораторіях світу ведуться роботи по вдосконаленню та оптимізації існуючих ДОФ, а також розробка нових ДОФ, характеристика яких задовільняє КРК.

Різноманітні ДОФ випромінюють статистичні характеристики, вимірювання яких порівнюється з відповідними характеристиками ідеально ДОФ і дозволяє зробити висновок про якість джерела і можливість його застосування для КРК. Зазвичай такі характеристики генеруючого реальним джерелом поля випромінювання.

Для ідеального ДОФ, який повинен генерувати поле з фоковим стано з точно визначеним числом фотонів n=1, середня кількість фотонів так само дорівнєю 1, дисперсія дорівнює нулю, а кореляційна функція також дорівнює нулю. Остання умова відповідає антигрупуванню фотонів, які випромінюються ідеальним однофотонним джерелом. Якшо відправити поле в однофотонному фоковському стані на зеркало (50% прозорості) і помістити на нього два детектори, то на них не зможемо спостерігати одночасних відліків, оскільки хвилева функція буде коллапсованою тільки на одному з детекторів[3]. Генерація випромінювання з вказаними статистичними характеристиками є досить складною експериментальною задачею. В імпульсному випромінюванні звичайних теплових джерел, які характеризуються розподіленням Бозе-Енштейна, а також випромінюванням одномодових лазерних джерел, які

генерують світло в когерентному стані і характеризуються Паусонівським розподіленням, поряд з необхідними в квантовій криптографії однофотонними імпульсами завжди є пусті імпульси і багатофотонні імпульси.

Найбільш близькими до ідеально ДОФ є джерела основані на використанні в якості випромінювачів одиночних квантово-механічних систем. При неперервному збудженні спускання такими квантовими системами світло є антигрупованим і складається з одиночних фотонів, розділених випадковими часовими інтервалами, тривалість яких залежить від часу життя збудженого стану і швидкості накачки. Типова кореляційна функція $g^2(\tau)$ інтенсивності флуоресценції одиночних квантових об'єктів, має провал до 0 при нульових затримках, який є результатом зменшення до нуля ймовірності одночасного випускання одиночною квантовую системою двох фотонів, внаслідок того, що при випусканні першого фотона система з визначеністю знаходиться в основному квантовому стані і навіть при сильному збудженні їй потрібен деякий час для того щоб, вона випустила наступний фотон.

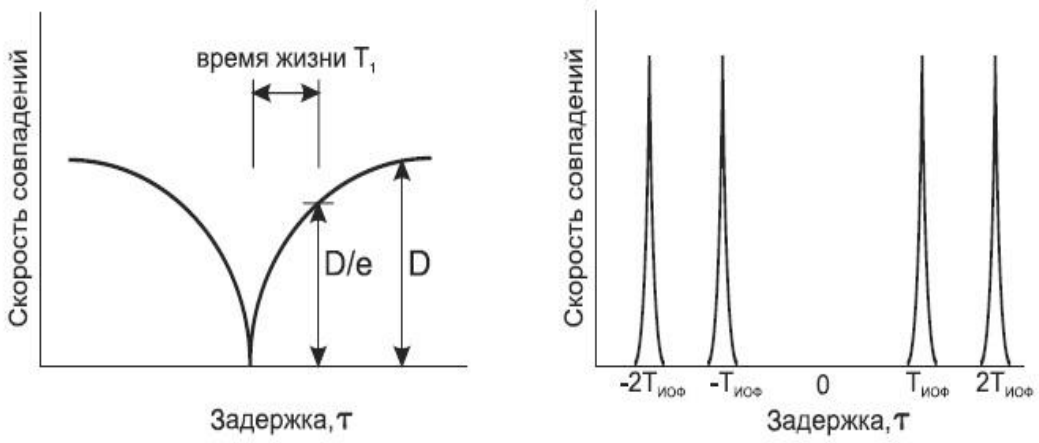

Рисунок 3.2 Вигляд кореляційної функції інтенсивності флуоресценції одиночного кванового джерела під час неперервного і імпульсного збудження.

З рисунка видно ширину провалу в кореляційної функції одиночного квантового джерела, визначається часом життя збудженого стану T_1.

Експериментальна реєстрація антигруповки фотонів, тобто провал до нуля є доказом того, що випущене випромінювання дійсно генерується одиночним квантовим випромінювачем [10]. Під час збудження одиночної квантової системи порядком коротких імпульсів кореляційна функція інтенсивності флуренційності має вигляд, представлений на рисунку. Особливість – відсутність так само як у ідеального ДОФ піку під час нульовій затримці τ. Варто відмітити, що по ряду причин для реальних джерел субпуасонівського випромінювання зазвичай спостерігається малоамплітудний пік під час невеликих затримок $\tau = 0$.

3.2. Детекрування одиночних фотонів

Відомо, що при наднизьких температурах матеріали переходять в надпровідний стан, які характеризуються наявністю куперівських електронних пар з низьким зв'язком між компонентами. Енергію фотона в інфрачервоному – діапазоні (ІЧ) достатньою, щоб зруйнувати велику кількість куперівських пар, вимірюючи тим самим електричні властивості надпровідних матеріалів. Детектори одиночних фотонів на надпровідних матеріалах мають в широкому діапазоні електромагнітного спектру: починаючи від гамма-випромінювання до інфрачервоної області. Практично будь-який тип таких детекторів може дозволити розширити кількість фотонів в імпульсі, який поступає. Недоліком таких систем є те, що їх потрібно охолоджувати до наднизьких температур, саме це ставить під сумнів використання таких систем на ринку з точки зору швидкодії [11].

Надпровідний тунельний перехід. Структура типу «надпровідник-ізолятор-надпровідник», яка знаходится при більш низькій температурі, ніж та, яка поступає в надпровідний стан. В якості матеріалу використовуюь ніобій, алюміній або оксид алюмінію. Принцип дії: поглинутий фотон викликає

руйнування куперівських пар в металі, в результаті чого утворюються квазічастинки. Якщо прикласти до структури невелику напругу – квазічастинки починають тунелю вати через ізолятор, створюючи струм, пропорційний поглинутій енергії. Якщо час існування квазічастинок більше ніж тунелювання, то вони встигають декілька разів тунелю вати в прямому та зворотньому направленні, створюючи додатковий вклад в вихідний сигнал. Недолік – окрім низької температури, великий «мертвий час» через що швидкість фотона не перевищую декількох кілогерц.

Надпровідний однофотонний болометр. Базується на принципі болометра, коли проходить значна зміна в опорі зразку при вивільненні невеликої кількості енергії в надпровідному шарі. Є два види таких приладів – сенсори граничного переходу і горячий електронний болометр.

Сенсор граничного переходу. В приладі використовується властивість деяких металів, які мать різкий перехід від звичайного стану до надпровідного, коли зміна температури на 1 мК достатньо, щоб метал змінив свій стан. Принцип дії: до металу, який знаходиться в надпровідному стані при температурі, близькій до критичної, прикладають невелику напругу, тому поглинання фотона такою структурою викликає невеликий струм, що веде до нагрівання і порушення надпровідного стану. Останнє характеризується підвищенням опору згідно з законом Джоуля-Ленца, кількість теплоти яка виділяється структурою зменшується, що приводить до охолодження і повернення металу в надпровідний стан, коли він знову готовий до прийому наступного фотона.

Резонансний контур. Тонка металічно надпровідна плівка є складовою мікрохвильового резонатора. Поглинання фотону призводить до появи квазічастинок і зміні повного опору прикладу і відновідно його індуктивності, що викликає зміщення резонансної частоти резонатора.

Гарячий електронний болометр. Найпростіший прилад, який окрім надпровідних матеріалів має геометрію типу «меандр», в якому підримується струм нижчий ніж критичний.

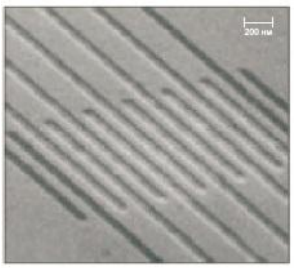

Рисунок 3.3 Фотографія геометрії надпровідної плівки в горячому електронному болометрі.

Вхідний фотон руйнує велику частину куперівських пар, створюючи локальну область підвищеного опору, тобто «гарячу точку», яка розтає, допоки не достигає край надпровідної плівки, ширина плівки досить мала, то після проходить розрушення надпроводимості по всій ширині плівки, яке викликає підвищення напруги на зразку, тобто викликає реєстрацію фотона.

Використання квантових точок – перспективне направлення в задачі реєстрації фотонів. Відмінність квантових точок від фотоелектричних перемножувачів (ФЕП) і лавинних фотодіодів (ЛФД) складається за відсутності внутрішнього механізму посилення, що дозволяє запобігти породження шуму, обумовлених наявністю електронної лавини і високої напруги живлення. Квантові точки – напівпровідникові структури нано розмірів, головною особливістю яких є дискретність електронного спектру, який виникає внаслідок потенційних енергетичних бар`єрів по трьох вимірах. Інколи квантові точки називають штучними атомами. Кількість енергетичних рівнів і електронів в квантовій точці залежить від її форми і розмірів – може бути виміряно.

Можливість керування додаванням у видаленням електронів з квантової точки виконується виміром прикладання напруги, заповнення енергетичних

рівнів електронами проходить в повній відповідності аналогічному процесу заповнення оболонок в атомі: на першій оболонці – два електрона, другій – чотири і т.д.

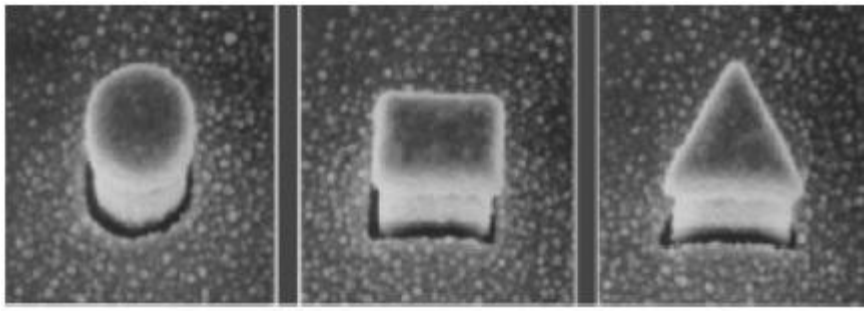

Рисунок 3.4 Види квантових точок.

Для задач квантової криптографії необхідні квантові точки такого розміру, щоб вони могли вміщати декілька електронів, для цього використовується структура не більша 0,01 мкм у всіх трьох вимірах. Для проведення такої маніпуляції існує декілька методів. Метод травлення – коли в напівпровідниковому матеріалі (кремній) протравлюються два вузьких канали на відстані 0,01 мкм один від одного. Кремній має чотири електрони на зовнішній оболонці, тому він прагне створити хімічну реакцію з іншими атомами для заповнення валентної оболонки. Але для поверхні атомів не завжди існує можливість створення такого зв'язку, тому для заповнення своїх зовнішніх оболонок вони використовують вільні електрони, створюючи надлишок негативного заряду на поверхні між протавленими каналами. Негативний надлишковий заряд витісняє вільні електрони, які залишились, до центру структури. Таким чином рух електронів обмежено центральною віссю, тому отримав структуру, яку називають квантовий дріт. Для створення масиву квантових точок необхідно протравити необхідну кількість аналогічних каналів в перпендикулярному направленні.

Другий метод – заснований на вирозуванні двомірної напівпровідникової плівки с великим поверхневим натягом на напівпровіднику з іншою

постійною решіткою, для прикладу, InAs на GaAs. Під час досягнення поверхневого натягу, на поверхі вирощуваного шару виникають невеликі нанометрові структури – квантові точки. Щільність квантових точок, які отримують таким методом буває доволі високою.

Для створення детектора одиночних фотонів з використанням квантових точок необхідно отримати струкруту, зображену на рисунку.

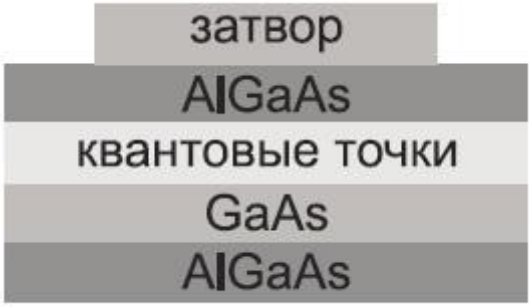

Рисунок 3.5 Структура детектора одиночних фотонів на основі квантових точок.

Два шари AlGaAs логуються таким чином, щоб отримати напівпровідник n-типу. Внаслідок того, що ширина забороненої зони GaAs менше, ніж у AlGaAs, електрони проникають в шар GaAs і забезпечують проводимість між витоком і стоком. Завдяки напрузі на затворі регулюється кількість електронів в канаді і відповідно його проводимість. Особливість даної структури - наявність шару квантових точок. Частина електронів з каналу переходить в незаповнені дискретні енергетичні рівні квантових точок. Хоча зв’язані електрони не можуть брати участь в проводимості, вони можуть впливати на неї шляхом електростатичної відштовхуючої взаємодії на електрони в каналі. Внаслідок чого в каналі виникають випадково розподілені потенціальні бар’єри і його проводи – зменшується.

Одиночний квант світла може поглинутись каналом, внаслідок чого в зоні проводимості утворюється електрон, а у валентній зоні – пустота. Збільшення

на одиницю числа електронів в каналі не призводить до помітного збільшення проводимості канала, який в середньому має близько 500 електронів. А пустота може тунелювати в найближчу квантову точку, де проходить процес рекомбінації і відповідно зменшення кількості електронів у цій квантовій точки на одиницю, що призводить до зниження електростатистичного відштовхування в області канала. Повернення детектора в початкове положеня проходить шляхом регулювання прикладеної до затвору напруги.

Існує ряд недоліків, які обмежують використання даного типу детекторів. Насамперед, мала величина квантового виходу, близько 1-10%, зв'язані з розміром каналу, внаслідок чого він майже прозорий для фотонів. Необхідність охолодження до 70 К, при більш високій температурі електрони можуть отримати достатню енергію, щоб покинути квантову точку. Вирішення цієї проблеми – створення квантових точок з глибокими енергетичними рівнями. Наступна проблема – мала швидкодія – не перевищує 100 Гц.

3.2.1. Фотоелектронний перемножував

Фотоелектронний перемножувач представляє собою електровакуумний прилад, в якому потік електронів, емітуємий фотокатодом під дією оптичного випромінювання, підсилюється в перемножувальній системі в результаті процесу вторинної електронної емісії [3]. Найбільш розповсюджені фотоелектронні перемножувачі, в яких підсилення потоку електронів здійснюється за допомогою декількох спеціальних електродів зігнутої форми – дінодів, що мають коефіцієнт вторинної емісії більше 1. Для фокусування і прискорення електронів на анод і діноди подається висока напруга – 600-3000 В. Інколи застосовується магнітне фокусування або фокусування в схрещеному електричному і магнітному полях.

Розрізняють декілька систем дінодів – жалюзійна, лінійно-сфокусована, кругова, венеціанське вікно. Вибір системи дінодів впливає на габаритні розміри фотоперемножувача, коефіцієнт підсилення, часові параметри, лінійність, чутливість до магнітних полів. Для прикладу ФЕП з лінійно-сфокусованою системою дінодів має хорошу лінійність і високий коєфіцієнт підсилення, завлячи чому широко використовується в спектрометрії. ФЕП з жалюзійною системою дінодів володію значно меншою лінійністю і більше повільними часовими характеристиками, але завдяки відносно низькій вартості вдало використовуюсь в осциляторних детекторах.

Фотокатоди ФЕП виготовляють з напівпровідників на основі з'єднання елементів 1 і 3 групи періодичної системи Менделеева з елементами 4 групи. Розрізняють декілька типів фотокатодів –біщілочний фотокатод (bialkali, K-Cs-Sb) для роботи в синій і зеленій області спектру з низьким темновим струмом, біщілочний фотокатод легірований рубідієм (rubidium bialkali, Rb-Cs-Sb), має підвищену чутливість в синій і зеленій областях спектру, але з подвійним темновим струмом. Мультищілочний фотокатод (multialkali S20, Na-K-Cs-Sb), з розширеною чутливістю від ультрафіолетовох до інфрачервоної області спектру, але потребує охолодження для зниження темнового струму. Високотемпературний біщілочний фотокатод (high temperature bialkali, Na-K-Sb), рекомендований для роботи при температурі більше ніж 60° С. Сонячно-сліпий фотокатод (solar blind, KBr, CsI, RbTe, CsTe) - призначений для роботи тільки в ультрафіолетовій області спектру.

Напівпрозорі фотокатоди зазвичай встановлюють на поверхню вхідного вікна скляного балону ФЕП. Для виготовлення дискретних дінодів використовують наступні матеріали: Cs3Sb, наносять в вигляді шару на металічну підкладку; сплави CuBe, CuAlMg; епітаксальні шари GaP на Mo, оброблені O_2 і інші. Канали неперервних дінодів виготовлюють зі скла з високим вмістом свинцю.

Матеріал вхідного вікна ФЕП визначає також визначає робочий спектральний діапазон фотоумножителя. Традиційно застосовуються такі скла - боросилікатне скло являє собою недороге скло для роботи з довжинами хвиль більше 260 нм; ультрафіолетове скло розширює чутливість до 180 нм; кварцове скло має прозорість до 160 нм; Флорид магнію пропускає ультрафіолетове випромінювання до 110 нм.

До основних параметрів ФЕП відноситься світлова анодна чутливість (відношення анодного фотоструму до викликає його світловому потоку при номінальних потенціалах електродів); спектральна чутливість (рівна спектральної чутливості фотокатода, помноженої на коефіцієнт посилення помножувальні системи; темновой ток (струм в анодному ланцюзі під час відсутності світлового потоку).

Застосування фотоелектронних помножувачів: хемілюмінесценція, біолюмінісценція, флуоресценція проточна цитометрії, хромотографи, аналіз стану навколишнього середовища, дозиметрія і радіометрія, дослідження космосу і астрономія,конфокальна і електронна мікроскопія, ядерна фізика та фізика високих енергій,гамма-каротаж і дифрактометрія.

Рисунок 3.6 Фотоелектронний перемножувач

Принцип дії. Одиночний фотон під час взаємодії з матеріалом катода створює фотоелектрон, який прискорюється електричним полем і рухається від

одного дінода до іншого, породжуючи електронну лавину. При цьому досягається значна величина фотоку, яка легко вимірюється. Але такі прилади мають свої недоліки.

Існує проблема вибору товщини катода. Занадто велика товщигна приводить до того, що електров в ряді випадків буде мати не достатньо енергії, щоб покинути поверхню катода. Або навпаки, тонкий катодний шар буде практично прозорий для фотонів, енергія яких перевищую задану величину. Товщина катода виконує важливу роль в обмеженні величини квантового виходу [12]. Для ФЕП також актуальна після імпульсові проблема – помилкового спрацювання детектора під час відсутності на вході фотона. Це трапляється через де іонізацію іонів і релаксації збуджених атомів, виникнувши в результаті проходження електронної лавини, які створюються в вакуумній трубці після проходження електронної лавини.

ФЕП мають відносно великі розміри, високу напругу живлення і підвищену чутливість до електромагнітного випромінювання і механічним вібраціям.

Загалом ФЕП – надійний прилад, який забезпечую стійку роботу в межах своїх можливостей. Також ФЕП один с перших детекторів, який зявився на ринку.

3.2.2. Лавинний фотодіод

Лавинні фотодіоди – лавинні фото провідникові діоди, які включені схемою зворотнього зміщення, режим роботи пов'язаний з наявністю напруги пробою на зворотній гілці вольт-амперної характеристики (ВАХ) напівпровідникового діода.

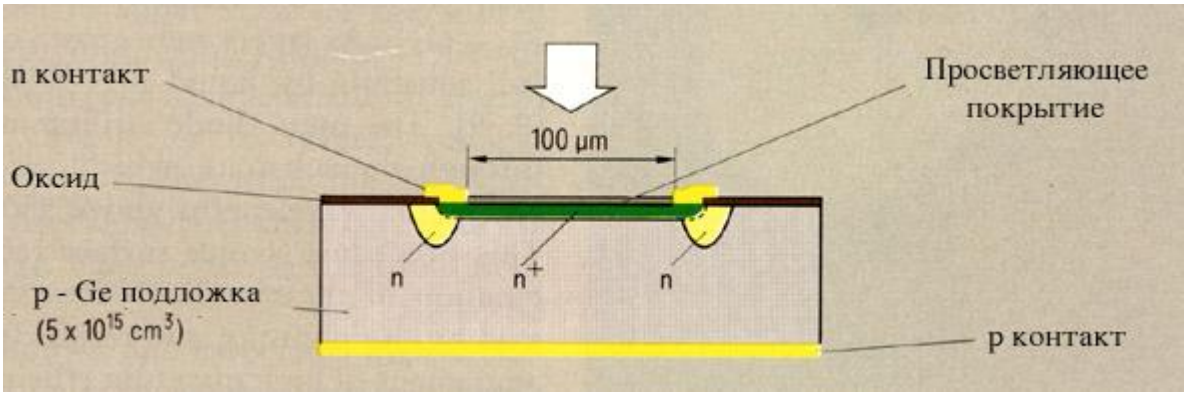

Рисунок 3.7 Лавинний фотодіод.

Існують два режими роботи лавинного фотодіода: лінійний режим, коли робоча напруга трохи нижче напруги пробою, і режим Гейгера, коли робоча напруга перевищує величину пробійної [13]. У першому випадку отримується посилення, зазвичай недостатньо для ефективної реєстрації одиночного фотона, тому більш широко застосовується другий режим. Однак при цьому повинен існувати обмежуючий механізм, який контролюючий електронну лавину і сприяє поверненню в початковий стан, а також запобігає помилковому спрацьовуванні детектора. Такий механізм реалізується двома способами: шляхом зменшення величини напруги нижче значення напруги пробою відразу після початку або під час реєстрації електронної лавини і шляхом використання режиму роботи, коли повідомляє прибуття фотона і напруга зсуву стає більше напруги пробою тільки на короткий проміжок часу, достатній для реєстрації фотона. Останній режим найбільш ефективний в боротьбі з темновими відліками, але він не вирішує проблеми посляімпульсів, коли відбувається спрацьовування фотодетектора при перевищенні робочої напруги вище напруги пробою в відсутності фотона. Явище послеімпульсів може бути викликано причинами: термічне збудження, туннелювання і ефект емісії захоплюючих центрів. Для запобігання даного ефекту необхідно зниження температури приладу і збільшення часу релаксації.

Виготовляють ЛФД з різних напівпровідникових матеріалів: Si, Ge, InGaAs, InP, GaAs, GaP, GaAsP, тому лавинні детектори широко використаються.

Також існує порядок деяких специфічних детекторів, використовуючи фотодіоди.

Гібридний детектор (hybrid detector). Поєднує в собі ФЕП і ЛФД з використанням напівпрозорого катода на вході. На першій стадії вільний фотоелектрон значно прискорюється і потрапляє в ЛФД, який грає роль вторинного підсилювача. При цьому досягається дуже мала, але достатня для реєстрації одиночного фотона, ступінь посилення.

Модуль для рахунку одиночних фотонів (single-photon counting module). Організовує рахунок фотонів, використовуючи набір кремнієвих ЛФД.

Пристрій із зарядовим зв'язком для підрахунку фотонів (Photon counting charge coupled device). Являє собою набір звичайних діодів. На відміну від інших детекторів, згенерована лавина електронів використовується для заряду ємності. Користувач може вираховувати інтенсивність світла, пропорціональну заряду на ємності. Через необхідність використання конденсатора, прилад має низьку швидкодію, яке в перспективі не зможе перевищити 10-100 кГц [3].

3.3. Типи кодування

3.3.1. Поляризаційне кодування

Поляризаційні схеми використовуються в вільному середовищі, де зберігається поляризація, але набагато важче їх встановлювати на оптичних хвилеводах через деполяризацію та випадково флуктуючого дволучепереломлення. Деполяризація це не основна проблема, її дію можно подавити за допомогою достатньо когерентного джерела. Часова шкала

флуктуації являється повільною. Одна не зважаючи на такі повільні флуктації можна спостерігати і більш швидкі, які роблять невожливим передачу ключа. Електронна система компенсації, виконує неперервне відстеження і виправлення поляризації, але вона потребую додаткової процедури узгодження мід Алісою і Бобом, що робить квантову криптосистему занадно громіздкою.

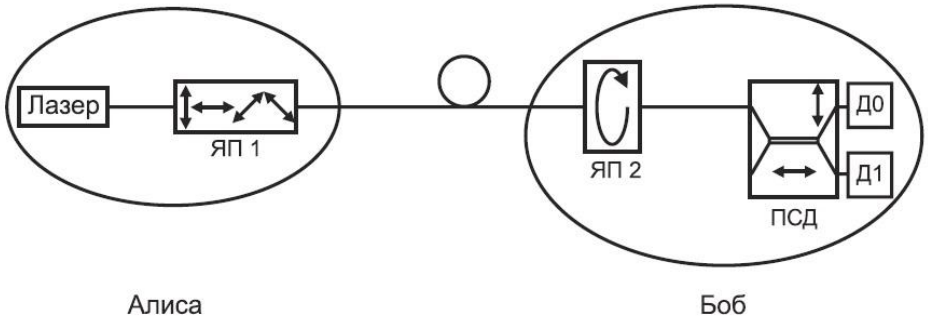

Рисунок 3.8 Поляризаційна схема, відправник Аліса пересилає Бобу слабкі імпульси поляризованого.

Поляризація управляється ячейка Поккельса (ЯП), яка дає Алісі можливість вибрати між 4 можливими поляризаціями: $|\updownarrow\rangle$, $|\leftrightarrow\rangle$, $|\nearrow\rangle$, $|\searrow\rangle$. На стороні Боба є ще одна ячейка Поккельса, яка контролює поворот схеми: 0° відповідає виміру в $\oplus$ - базис, 45° відповідає виміру в $\otimes$ - базисі. Поляризаційний світо дільник (ПСД) розділяє промінь на два ортогональні компоненти, які реєструються детекторами Д0 і Д1 [3].

3.3.2. Фазове кодування

Фазове кодування з інтерфереометром Маха-Цандера. Для того, щоб надіятись на поляризацію, яку нелегко контролювати в оптичних хвилеводах, доречно використати систему КРК при фазовому кодуванні [14]. Схема являє собою розгалужений інтерферометр Маха-Цандера з двома фазовими модулями

(ФМ), яки дозволяють зробити кодування та декодування. Уявимо, що Боб не використовує свій ФМ і схема налаштована таким чином, щоб створювати конструктивну інтерференцію на детекторі Д0 і деструктивну на детекторі Д1. Якщо Аліса використовую свій ФМ для того, щоб здвиг фази величиною 0 або π, то Боб отримає відлік на Д0 або на Д1. Це еквівалентно поляризаційній схемі кодування, в якій використовується дві поляризації. Щоб достигнути конфіденційності, додається випадковий вибір базиса. Аліса повинна вибрати один з чотирьох здвигів фази 0, π або $\pi/2, 3\pi/2$. Зі своєї сторони Боб також вибирає між нульовим здвигом фази в $\pi/2$, тобто вимір в $\otimes$ - базисі. Така схема еквівалентна поляризаційній схемі кодування в протоколі BB84.

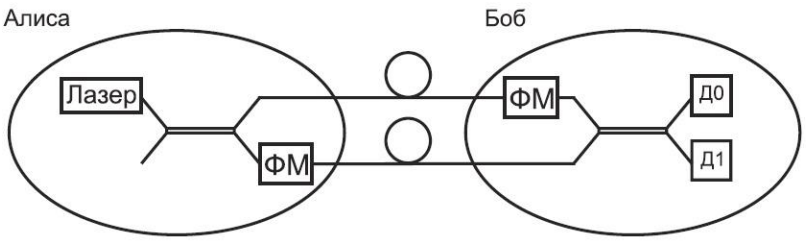

Рисунок 3.9 Схема фазового кодування з використанням інтерформетра Маха-Цандера

Відносний вибір фази в двох фазових модуляторах ФМ створює інтерфераційну картину. Адіса вибирає одну з чотирьох фаз 0 або π, що відповідає забису $\oplus$, або $\pi/2, 3\pi/2$ - відповідає $\otimes$ - базису. Коли Аліса і Боб використовують один і той самий базис, відлік на Д0 означає 0, а відлік на Д1 – 1. В таких же випадках, коли базиси н відрізняються, немає ніяких кореляцій між бітом, відправлений Алісою і тим який отримав Боб.

Фазове кодування подвійним інтерферометром Маха-Цандера. Зберігання різності фаз в розгалуженому інтерфометрі дуже складно.

Відповідно з практичною точки зору краще використовувати інтерфометр зображений на рисунку.

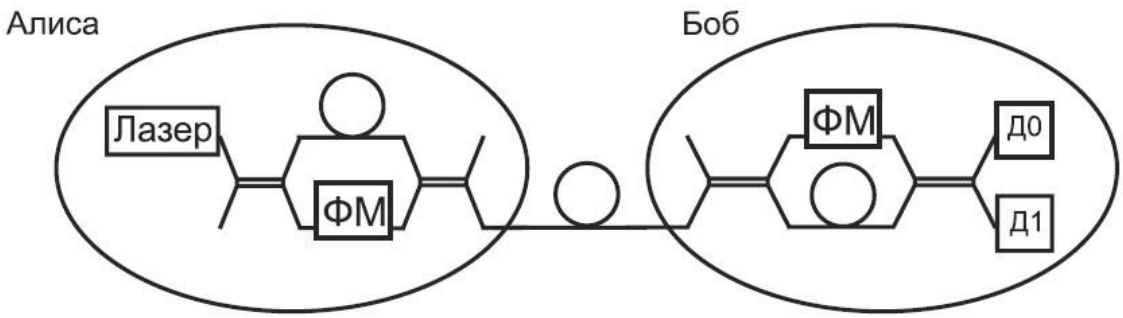

Рисунок 3.10 Схема фазового кодування з подвійним інтерфометром Маха-Цандера

Імпульс згенерований лазером Аліси ділится на два. Отримавши імпульси, розповсюджуються один за одним, від Аліси до Боба, вздовж одного передаючого світловода проходять короткий і довгі шляхи. Після проходження через інтерфометр Боба з них виходять 3 імпульси. Два з них позначаються як, коротки-короткий і довгий-довгий не важливі, зважаючи на те що вони не приводять до інтерференції. В той самий час центральний імпульс відповідає двом важливим шляхам: короткий-довгий або довгий-короткий, які не розрізнюються і відповідно інтерферуються. У той же час центральний імпульс відповідає двом можливих шляхів: короткий-довгий або довгий-короткий, які невиразні, отже интерферируют. Вибір фазових руйнувань, створюваних Алісою і Бобом, відповідає кодуванню або декодуванню. Очевидно, що така схема більш стабільна, ніж попередня. Оскільки два когерентних вклади згодом поділяються лише на кілька фемтосекунд, поширюючись при цьому по одному волокну, то вони не піддаются ніяким температурним або механічним флуктуаціям. Різниця оптичних шляхів в розбалансованні інтерферометра Боба повинна бути такою ж, як і в інтерферометрі Аліси і залишатися постійною з

точністю до часток довжини хвилі. Однак, вимагає лише ретельної локальної температурної стабілізації двох інтерферометрів. Недолік схеми полягаєв тому, що ми втрачаємо половину сигналу в імпульсах довгий-довгий і короткий-короткий

"Plug & Play" криптосистеми з самокомпенсацією. В наш час налаштований комерційний випуск фазових модуляторів для телекомунікаційних довжин хвиль, що робить вибір на користь стандартних фазових кодуючих систем при реалізації каналів на основі оптичного волокна. В таких схемах також необхідно ретельне поляризаційне узгодження. В двох розбалансованих інтерферометрах Маха-Цандера поляризація повинна встановлюватися так, щоб интерферируючі компоненти мали однакову поляризацію на вихідному світлодільнику Боба. Після вихідного узгодження блоків Аліси і Боба все повинно бути стабільно і не викликати ніяких проблем. Серйозна проблема зумовлена тим фактом, що фазові модулятори виготовлені з електрооптичних кристалів, які забезпечують лише один з двох напрямків поляризації. Для того щоб уникнути флуктуації інтенсивності на виході у Боба, через модулятор можна пропускати лише одну певну поляризацію. Це повертає до необхідності управління приходячою поляризацією. Але в такій системі як "Plug & Play", запропоновано і реалізовано в роботі, немає необхідності постійного узгодження поляризації у волоконно передавальной лінії [15]. Ідея полягає в тому, що світловий імпульс випромінюється не Алісою, а Бобом; імпульс спочатку поширюється до Аліси, де він модулюється, а потім відбивається назад до Боба. Якщо відбивачі зроблені на основі дзеркал Фарадея, то поляризації інтерферуючих компонентів на виході Боба завжди узгоджені між собою. Фарадеевське дзеркало - 45° ротатор Фарадея і видбиваюче назад дзеркало, формує відображену поляризацію ортогональну поляризації світла, що направляється в волокно; таким чином, будь-які зміни

поляризації вздовж лінії передачі або всередині інтерферометра ефективно подавляються.

Система реалізує на основі протоколу BB84 з чотирма станами, показана на рисунку і розглядається в работе. В цьому експерименті роль лінії передачі грав стандартний телекомунікаційний оптоволоконний кабель довжиною 23 кілометрів. Без будь-якої активної стабілізації був отриманий рівень помилки менше 1% при рівні формуванні мережевого ключа 210 Гц. Під час всіх експериментів на довжинах телекомунікаційних хвиль приблизно 1300 нм основна частина шуму була викликана високим фоном темнових відліків в однофотонних детекторах. Саме з використанням "Plug & Play" криптосистем пов'язані останні досягнення в забезпеченні надійного КРК на граничних відстанях, що визначаються втратами в оптоволокні

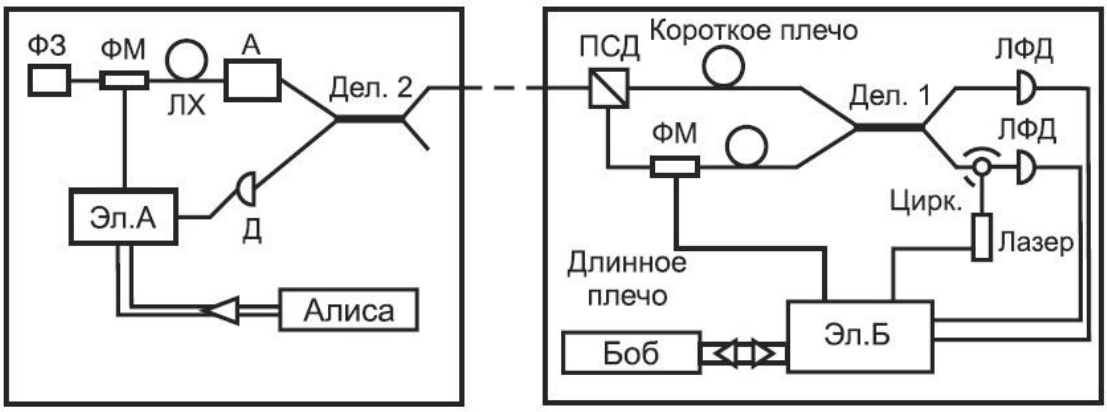

Рисунок 3.11 Принцип квантовії криптографічнох системи "Plug & Play"

Боб відправляє світловий імпульс через циркулятор. Цей імпульс розщеплюється на дільники 1. Перша половина направляється по короткому шляху. Контролер поляризації встановлюється таким чином, щоб цей імпульс повністю проходив через поляризаційний світло дільник ПСД. Потім він розповсюджується до Аліси, де знову розщеплюється на дільнику 2 для забезпечення сигналу синхронізації. Далі від проходить через апаратуру Аліси і віддзеркалюється назад до Боба. Завдяки дії фарадеївського дзеркала

компенсується двопромінне переломлення оптичної ланки і імпульс повертається назад ортогонально поляризованим. Після цього відбивається ПСД і йде в довге плече, де Боб вводить фазовий здвиг за допомогою модулятора ФМ. Другий імпульс позвопсюджується по двом плечам в зворотній сигнал до однофотонного рівня А. Оскільки два імпульса розповсюджуються вздовж тих самих шляхів, він виявляється у дільника 1 одночасно з ідентичними поляризаціями, що приводять до інтерференції. Лінія зберігання ЛЗ введена в систему Аліси, щоб запобігти проблем пов'язаних з релеевським розсіюванням назад. Ел. А і Ел Б – електроніка Аліси і Боба для управління обміну даними [3].

Висновок з розділу 3

Джерела одиночних фотонів на основі послаблених лазерних імпульсів просто в використанні, наявність широкого ряду лазерів працюючих при кімнатних температурах і генеруючи випромінювання практично в будь-яких довжинах хвиль, легко маніпулювати, збирати і відправляти на потрібні детектори. Основними недоліками ДОФ є ймовірність того, що джерело може випустити декілька фотонів одночасно, а також температурний режим під час роботи приладу.

Традиційні пристрої детектування ФЕП і ЛФД є найбільш розповсюдженими в квантових системах, але не зважаючи на широке використання вони мають ряд недоліків пов'язаних не високою швидкодією внаслідок наявності в лінії шумів, тому ведуться досліди інших типів детекторів.

Поляризаційне і фазове кодування, які використовуються, але мають ряд недоліків, для усунення яких потрібні системи компенсації, яка буде неперервно відслідковувати і виправляти поляризації, що зробить систему на

порядок громіздкою. На данний час ведеться вдосконалення методів кодування в квантових системах.

РОЗДІЛ 4. КВАНТОВЕ РОЗПОДІЛЕННЯ КЛЮЧІВ НА БАГАТОФОТОННИХ СТАНАХ

4.1. Джерела когерентних станів

В якості джерела когерентних станів може використовуватись лазер, стабілізований по частоті і фазі, випромінювання якого в межах часу когерентності, описується когерентним станом гармонічного осцилятора. В відомих експериментах використовувався напівпровідниковий лазер, відносно простий і не дорогий. Частота припромінювання лежить в оптичному діапазоні 780, 810 нм і в мікрохвилевому 1,55 мкм [16, 17]. Лазер може працювати в неперервному стані і в імпульсному режимі, неперервне випромінювання лазера розбивається на імпульси довжиною 120 нс з частотою повторення 800 кГц за допомогою акусти-оптичного модулятора [16]. В останьому відомому експерименті імпульс мав приблизно 250 фотонів. Кожен імпульс переносить один символ ключа.

Для лазера потрібна трьорівнева структура. В ній необозв'язково повинно бути три рівні – може бути набагато більше. Далі в системі потрібно створити інверсну заселеність рівнів.

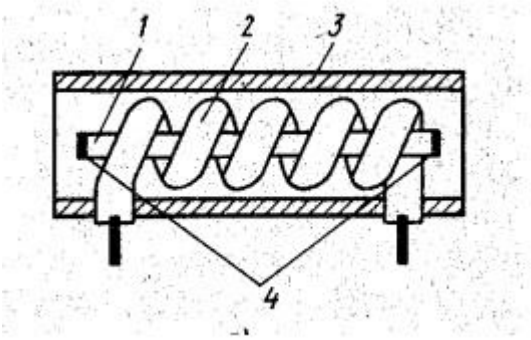

Рисунок 4.1 Схема рубінового лазера. 1 – активний елемент, 2 – спіральна лампа накачки, 3 – відзеркалювач, 4 – дзеркала резонатора.

В наш час існує багато лазерних середовищ, які можуть випромінювати лазерне випромінювання – тведрі, рідкі і газоподібні. Перше таке середовище знайти було доволі непросто. Перша вдала спроба була в 1954 році в Фізичному інституті Академії наук (СССР) Миколою Басовим і Олександром Прохоровим і в Колумбівському університеті (США) Чарльзом Таунсом, в 1964 році троє дослідників отримали Нобелівську премію по фізиці.

В якості речовини в цьому пристрої використовувався аміак. Але випромінював він не світло а радіочастотні хвилі і був названий Таунсом мазером. Завдяки особливості підсилювати радіохвилі мазери відразу почали використовуватись в радіотелескопах. Перший лазер був створений в 1960 році американським фізиком Теодором Мейманом. Робочим тілом в лазері був стержень з рубіна. Рубін представляє собою оксид алюмінію, який містить атоми хрому, що надають рубіну червоне забарвлення. Саме переходи в атомах створюють лазерне випромінювання рубіна по схемі, яка зображена на рисунку вище.

Сильним імпульсом світла від газорозрядної ксенової лампи накачки електрони в атомах хропа збуджуються з рівнім основного стану на рівні накачки, які створюють інверсну заселеність по відношенні з проміжними рівнями з енергією E_2. Примусові переходи електронів з рівна накачки на проміжні рівни викликають випромінювання світла в червоному діапазоні спектру довжини хвилі, приблизно 690 нм. Накачка здійснюється в імпульсному режимі, відповідно і випромінювання лазера імпульсне. З двох кінців рубінового стержня – створюючи нові фотони. Процес нарощується лавинно до тих пір коли світловий імпульс не вийде назовні через напівпрозоре дхеркало. Випромінювання рубінового лазера достатньо потужне, але не однорідне. Рубіновий кристал звісно може бути замінений іншим матеріалом, який має власні і домішки атомів, забезпечуючи генерацію випромінювання в

активному оптичному середовищі. Середовищем може служити – тверде, рідке або газоподібне тіло [20].

Принципіальною є можливість випромінювального переходу в матеріалі, використаному в якості лазерної матриці.

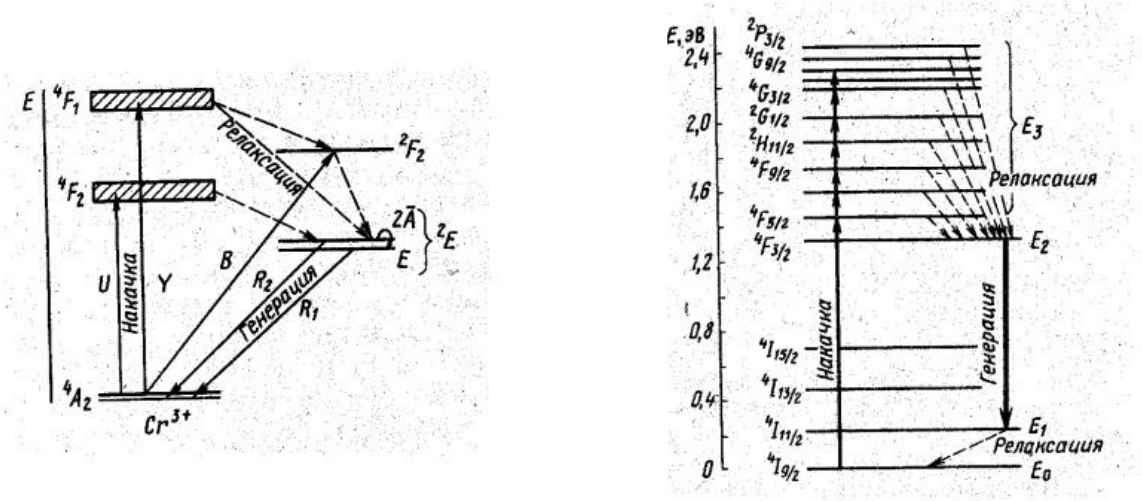

Рисунок 4.2 Діаграма енергетичних рівнів іонів Cr^{+3} в Al_2O_3(а) і Nd^{+3} в $Y_3Al_5O_{12}$ (б) і схема роботи лазера по трьорівненій системі (а) і чотирьохрівневій (б).

В групі твердих лазерів першим представником є рубіновий лазер, активним матеріалом служить кристалічний або аморфний діалектрик. З точки зору отримання лазерної матриці найбільш простими є скліні лазери, більш складними – лазери на олександриті. Зниження значення коефіцієнту корисної діх і високі енергії накачки рубінового лазера були подолані за допомогою використання в якості активатора іонів рідкоземельних елементів, побудованя енергетичних рівнів дозволяю забезпечити роботу по 4-х рівневій системі. В першому випадку (а) іон-активатор створюю в забороненій доні діалектрика електронні рівні, переходи електронів між обумовлюють:

1) поглинання енергіх або накачки;
2) релаксаціх або безвипромінювальні переходи;
3) люмінесценції або генерації випромінювання.

Таблиця 4.1 Основні матеріали і характеристики твердоті лих лазерів

Основные материалы и характеристики твердотельных лазеров

№ п/п	Материал активной среды			Длина волны генерации, мкм	Показатель преломления	Режим генерации излучения	КПД, %
	матрица	активатор					
		природа	концентрация мол.%				
1.	Рубин Al_2O_3	Cr^{+3}	0,03–0,05	0,694	1,76	свободный	1
2.	Иттрий-алюминиевый гранат (с неодимом) $Y_3Al_5O_{12}$	Nd^{+3}	1–3	1,06	1,83	непрерывный	4
3.	Стекло (с неодимом) (с эрбием)	Nd^{+3} Er^{+3}	2–6 1	1,06 1,54	1,55	свободный	8 3
4.	Алюминат иттрия (с неодимом) $YalO_3$	Nd^{+3}	3	1,06	1,95	непрерывный	1
5.	Натрий-лантан-молибдат (с неодимом) $NaLa(MoO_4)_2$	Nd^{+3}	2	1,06	1,82	свободный	2,5
6.	Флюорит (с диспрозием) CaF_2	Dy^{+3}	0,02	2,36	1,42	непрерывный	2
Перестраиваемые лазеры							
7.	Гадолиний-скандий-галлиевый гранат (с хромом) $Gd_3Sc_2Ga_3O_{12}$	Cr^{+3}		0,7–0,9	2	импульсный	2–3
8.	Сапфир Al_2O_3	Ti^{+3}	0,1	0,7–0,98	1,7	импульсный	3
9.	Александрит ($BeAl_2O_4$)	Cr^{+3}		0,7–0,82	1,75	импульсный	2–3
10.	Щелочно-галлоидные кристаллы NaCl, LiF, KBr, RbI и др.	F-центры	–	0,5–4 (от LiF до RbI)	1,54 (NaCl)	свободный	30

В наш час найбільш поширеним твердотілим лазер ж лазер на ітирій-алюмінієвій основі, завдяки низьким пороговим енергіям накачки, високій теплопроводи мості і твердості матриці, малим оптичним втратам, простоті індукції, високій потужності і частоті слідування імпульсів випромінювання (до 10 кГц). Загальним недоліком всіх матриць, активованих рідкоземельними металами є відстудність широких смуг поглинання. Тому для підвищення ефективності накачки аткі матриці, крім іонів-активаторів, вводять іони-сенсибілізатори. Наприклад, Cr^{+3}, поглинають енергію в шикорому спектральному діапазоні і віддають її іонам-активаторам. Важливе значення мають твердотілі перебудовувальні лазери, які довзоляють змінити довжину хвилі випромінювання в деякому діапазоні. Такі лазери використовують матеріали з широкими інтенсивними смугами люмінесценції. Ці лазери працюють в 4-х рівневій системі завдяки широким енергетичним рівням іонів-

активаторів і ефективній взаємодії цих іонів з коливання кристалічної решітки. Прикладом такої лазерної системи є монокристалічна матриця на основі александрита або хризоберила, в якому частина іонів Al^{+3} заміщена іонами Cr^{+3}. Менш важким є отримання матриць перебудованих лазерів на основі галогені дів щілочних металів, активованих F-центрами. F-центри створюються з точкових дефектів монокристала і обумовлюють широкі полоси поглинання випромінювання з наступною люмінесценцією.

Необхідна концентрація F-центрів в матриці складається за допомогою фотохімічной і термічною обробкою вихідного монокристалічного матеріалу. Поєднання в одному приладі лазерних матриць на основі різних галогені дів дозволяє перекривати широкий діапазон довжин хвиль, але ці матеріали мають низьку термічну і оптичну стабільність з робочою температурою приблизно 77 К [3]. Накачку таких лазерів виконують за допомогою іншого лазера відповідної довжини хвилі.

Цілком особливий клас твердотілих лазерів представляють напівпровідникові лазери. Вони відрізняються тим, що вони мініатюрні, високоефективні, легко управляються електронним способом, працюють на низьких напругах, стікі до механічних взаємодій і витоговляються по технологіх мікроелектроніки, тобто призначені для масового виготовлення тому і дешеві.

Основна ідея в роботі напівпровідникових лазерів заключається у використанні випромінювальної рекомбінації в напівпровідниках, яка призводить до лазерної генерації. Для цього необхідно матеріал з безліччю електронів в зоні проводимості, які намагаються її покинути і в той же час безліч дірок в валентній зоні готових прийняти ці електрони. Однорідний напівпровідник для таких цілей не потрібен тому, що в ньому не реалізується одночасно дві вказані умови. Але високу концентрацію електронів можна отримати в сильно легованому напівпровіднику n-типу, а високу концентрацію

дірок – в сильно легованому напівпровіднику p-типу. Якщо такі два напівпровідника поєднати разом, то в області p-n переходу можна одночасно реалізувати дві умови, необхідні для лазерної генерації.

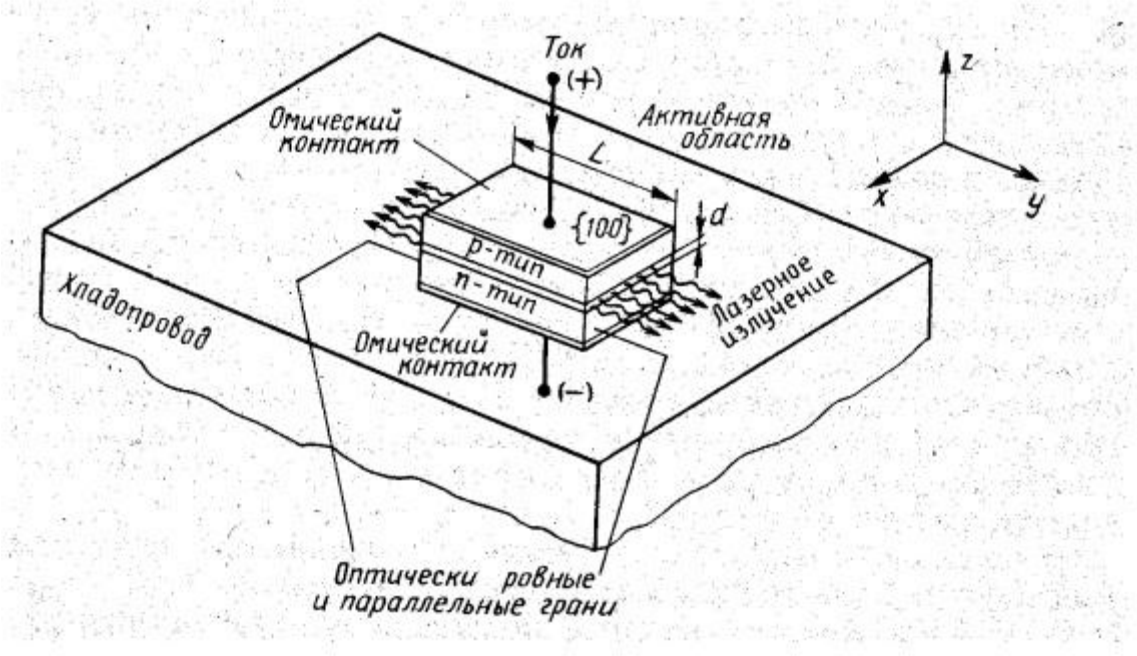

Рисунок 4.3 Схема напівпровідникового лазера.

Під час подачі на p-n перехід прямої напруги, то біля такого переходу з’являється область перекриття, де є великі концентрації електронів і дірок. Така область називається активною, тому що саме тут проходить інтенсивна випромінювальна рекомбінація електронно-діркових пар. Щоб підтримувати процес випромінювання, необхідно компенсувати рекомбінаційний спад носіїв заряду, пропускаючи через прилад електричний струм і тим самим інженеруючи в активній області нові носії. Таким чином, конструктивно напівпровідниковий інжекційний лазер схожий на звичайний напівпровідниковий діод на основі p-n переходу.

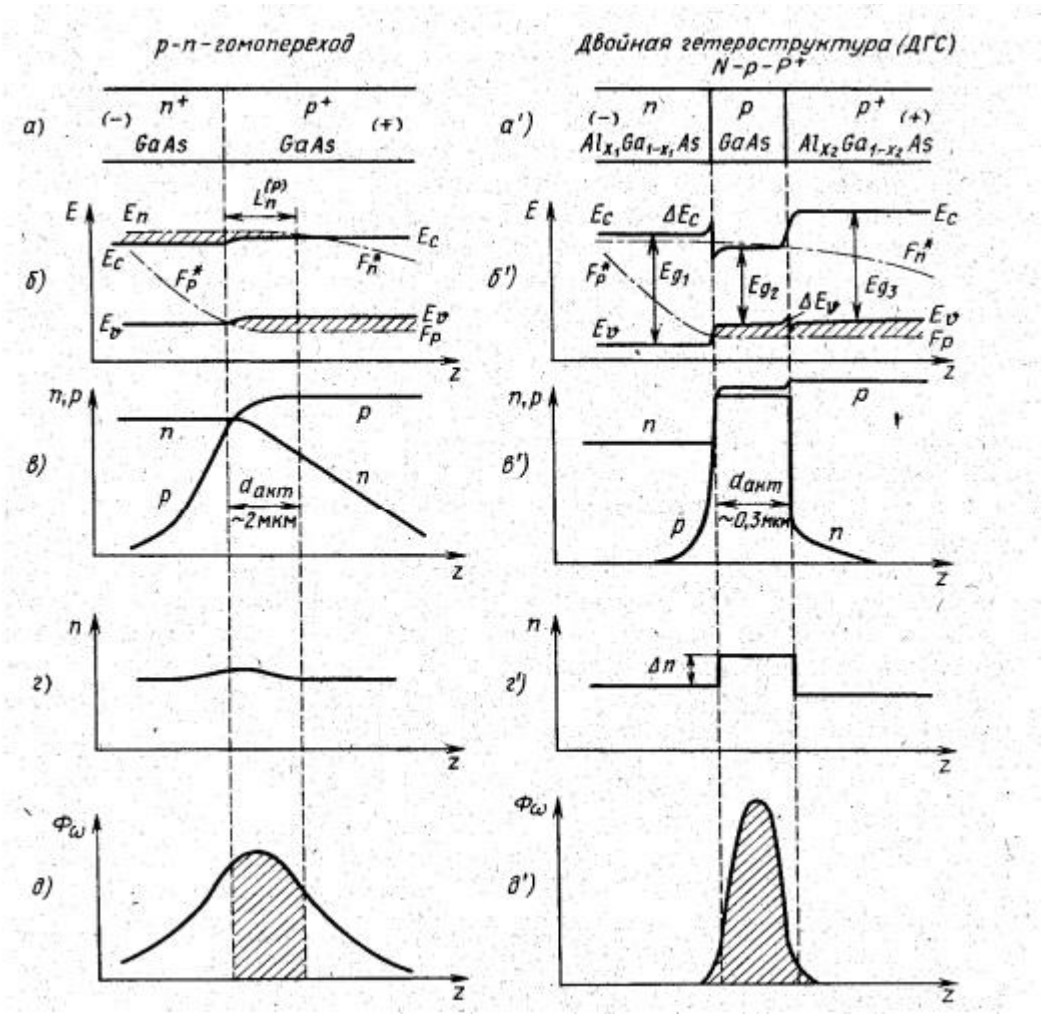

Рисунок 4.4 Порівняльні характеристики лазерних стуркур на основі гомо – і гетеропереходів: а) стукрутра; б) енергетичная діаграма; в) розподілення концентрації носіїв заряду; г) показник переломлення; д) розподілення інтенсивності випромінювання лазера.

Для забезпечення ефективної взаємодії світла з активним середовищем необхідно поєднати області інверсного заселення з областю розповсюдження світлового випромінювання, тобто локалізувати в одному шарі нерівносні носії заряду і фотону. В структурах на основі гомо переходів ця задача реалізується неоптимально, тому в даний час найбільша доля промислового випуску йде на інжекційні лазери на основі подвійних гетероструктур. В таких структурах ефекти односторонньої інжекції, над інжекції, хвильовий ефект дозволяють

значно полегшити досягнення стану інверсної заселеності в активній області. Зокрема за рахунок ефекту над інжекції концентрації електронів в активній області вище ніж в емітері. Разом з цим потенційний барєр на границі $p\text{-}p^+$ закриває електрони в межах вузької активної області гетероструктури. Аналогічно для дірок. Окрім розглянутого обмеження реалізується ефективне оптичне обмеження, оскільки показник переломлення різко змінюється на границях гетеропереходів і активний шар поводить себе як хвилевід, локалізуючи випромінювання в межах активної області.

Реальні напівпровідникові лазери на сучасному етапі розвитку квантової електроніки складаються в вигляді подвійних гетероструктурних або плоских подвійних гетероструктурних з розподіленим зворотнім зв'язком.

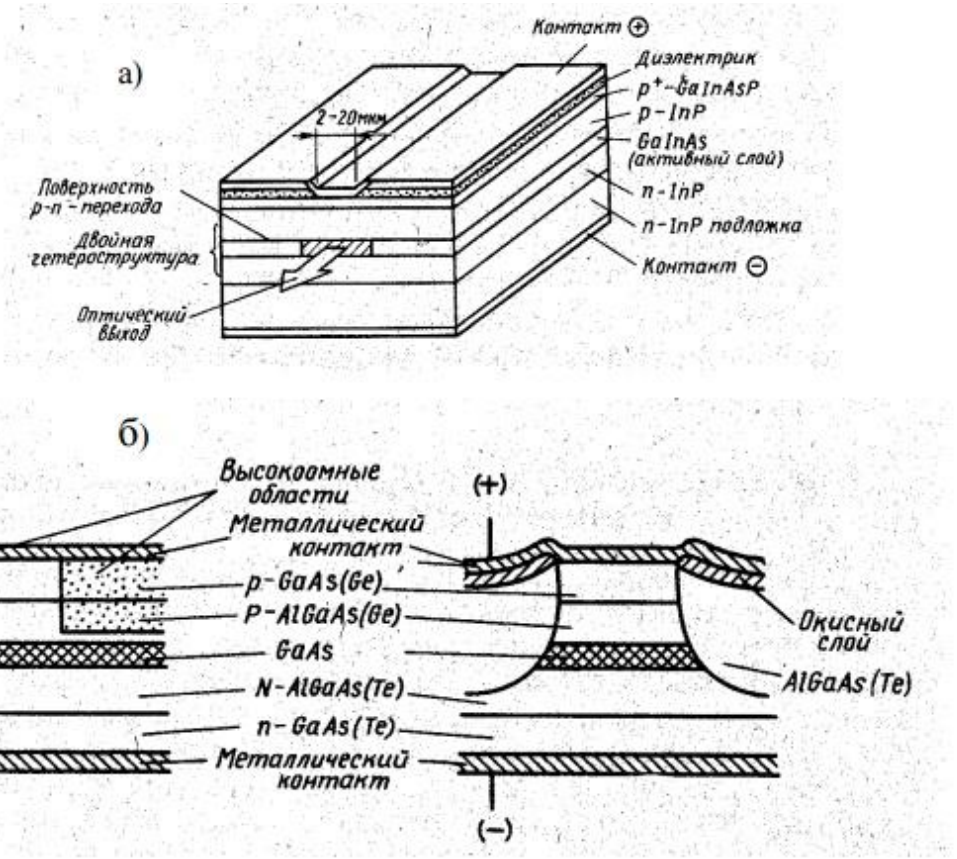

Рисунок 4.5 Структури контактних подвійних гетероструктурних-полоскових лазерів; а) контактова структура з однаковим обмеженням; б) ниткоподібна структура з двокоординатним обмеженням.

Склад напівпровідника визначає довжину хвилі і вибирається за умови з трьома областями пропускання оптичних волокон. Використовуючи тверді розчини різних складових, можна в широкому діапазоні варіювати характеристики інжекційних лазерів. Потужність яких в неперервному стані складає приблизно декілька Вт.

Таблиця 4.2 Довжини хвиль випромінювання в залежності від середовища

Склад активного середовища	Довжина хвилі випромінювання, мкм
$Al_{0,05}Ga_{0,95}As$ або GaAs	0,84
$Ga_{0,28}In_{0,72}As_{0,6}P_{0,4}$	1,3
$Ga_{0,4}In_{0,6}As_{0,88}P_{0,12}$	1,55

В подвійному гетероструктурному-плосковому лазері ширина активної області обмежена полосковим омічним контактом розміром близько 10 мікрон, що забезпечую зниження робочого струму і підвищую стійкість роботи лазера. В такій багатошаровій структурі міститься близько п’яти шарів, з яких три центральні створюють робочу подвійну гетероструктуру. Перший шар легірованого напівпровідника, нанесений на низькоомну підкладку, служить широкозонним N-емітером інжекційного лазера. Потім наноситься активний шар у вигляді твердого розчину ізоперіодичного підложку і далі формується широко зоновий Р-емітер. Останній напівпровідниковий високолегірований шар твердого розчину забезпечує якісний омічний контакт. Шар діалектрика відділяє напівпровідник від контакту за межами полоски. Такі структури забезпечують електронне і оптичне обмеження впродовж вісі z. Кращими характеристиками володії лазер з двокоординатним обмеженням і впродовж вісі z і в межах інжекційного p-n переходу.

Подальше вдосконалення характеристик інжекційного напівпровідникового лазера було досягнено в подвійних гетероструктурних лазерах з розділеним електронним і оптичними обмеженнями.

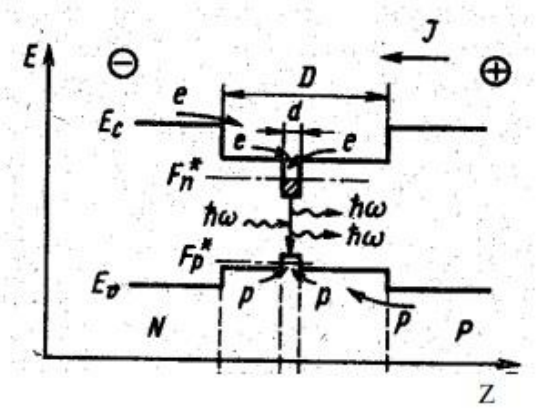

Рисунок 4.6 Схема роздільного оптичного і електронного обмеження

В таких структурах всередині тонкого активного шару d виконується електронне обмеження, а всередині товстого шару D – оптичне обмеження. Під час пропускання струму в прямому направленні електрони і дірки із широкозонних емітерів інжекціюються в товстий вузькозонний шар, а потім потрапляють в тонкий ще біль вузько зоновий активний шар, в якому проходить випромінювальна рекомбінація. В сучаних лазерах в якості тонких шарів (5-20 нм), де проходить скопичення нерівносних носіїв і їх випромінювальна рекомбінація, використовуються кванторозмірні стуктури (квантові ями). В кванторозмірних структурах в ролі характерної фізичної довжини, тобто довжини з якоє порівнюються розміри прикладу, виступають квантові величини. Для електронів в твердому тілі такою довжиною є довжина хвилі де-Бройля.

Якшо характерний геометричний виміряний розмір менше довжини хвилі де-Бройля для електрону, то проявляються ефекти розмірного квантування, тобто є характер квантування енергії електрона, її величина залежить не тільки від природи матеріалу, але і від розмірів. З цього випливає, шо енергією рівнів і

хвилевими функціями можна управляти, вимірюючи розміри об’єкта. Використання квантоворозмірних структур в активному шарі лазера дозволяє:

1) зменшити порогову щільність струму накачки;

2) послабити температурну залежність щільності струму накачки;

3) збільшити коефіцієнт підсилення випромінювання на одиницю довжини активної області;

4) покращити спектральні характеристики генеруючого випромінювання.

Структура лазера з квантоворозмірним активним шаром включає велику кількість тонких над тонких шарів. Ширина квантової ями в такій структурі складає 10 нм. Хвилевод включає чергуючи шари короткоперіодної надрешітки (СР) і широко зоновий шар $Al_xGa_{1-x}As$ змінного складу. При цьому над решітка представляє собою сукупність взаємодіючих квантоворозмірних ям, перекриття електронних станів в якій обумовлюється створенням дозволених мінізон, розділених забороненими зонами, як в твердому тілі.

Створення розподілених лазерів з подвійною гетерострукрурою потребують високого рівня технології отримання нанорозмірних монокристалічних шарів, для чого і використовується молекулярно-променева епітаксія з метолоогранічних зєднань і рідко фазова епітаксія.

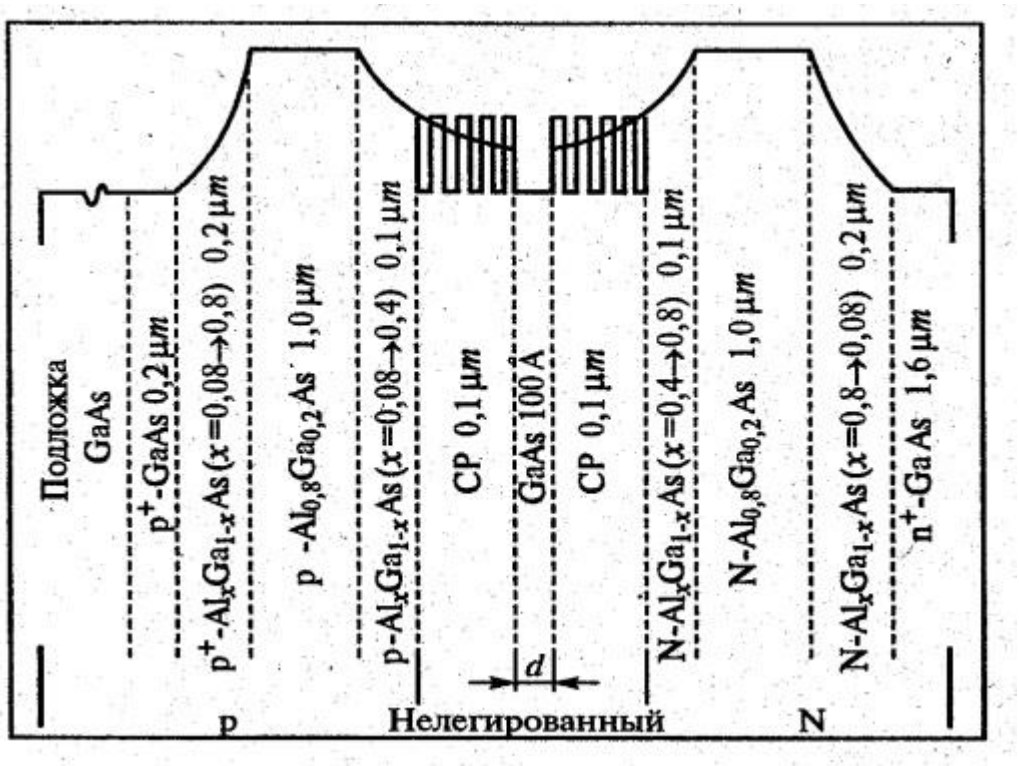

Рисунок 4.7 Структура розподіленого лазера з подвійною гетероструктурою, квантовою ямою і параболічним хвилеводом

Можливість створення лазерів на матрицях, які знаходяться не тільки в твердому, але і в рідкому і газоподібному станах. В 1960 році Алі Джаван, американський фізик іранського походження, створив перший газовий лазер. Зараз доволі розповсюджені малопотужні газові лазери на основі суміші гелія з неоном, випромінюючі на довжині хвилі 632 нм і використовувані для дослідних і метрологічних цілей, і потужні на основі CO_2, випромінюючі в інфрачервоному діапазоні на довжині хвилі 10,6 мкм і використовувані для технологічних цілей. Обидва типи лазерів випромінюють світло, на відміну від рубінового лазера, не в імпульсному, а в неперервному режимі.

В 1966 році Б. Степановим, А. Рубіновим і В. Мостовниковим в Інституті фізики АН БССР (Мінськ) були створені перші рідкі лазери на основі органічних барвників, які завдяки низькій вартості і можливості використання в

одному лазері набору барвників, випромінюючих на різних довжинах хвиль – отримали широке розповсюдження.

4.2. Середовище розповсюдження сигналу

В якості розповсюдження оптичного сигналу може використовуватись як відкритий простір, так і оптичне волокно, Техніка КРК на осві когерентних станів набагато менш чутлива до флуктацій поляризацій і втрат, ніж техніка одиночних фотонів. У всіх відомих експериментах використовувалась відправка світла в відкритому просторі, але немає ніяких підстав вважати, що використання оптоволокна приведе до принципіальних складностей.

Геометрична оптика розглядає випромінювання як тонкі пучкі світла – промені в однородному середовищі, які розповсюджуються прямолінійно. Геометрична оптика базується на чотирьох аксіомах:

1) промені світла розповсюджуються незалежно один від одного;
2) сумарна інтенсивність двох пучків дорівнює сумі інтенсивності кожного пучка при відсутності другого (суперпозиція). Порушення такої аксіоми супроводжується інтерференцією, випромінювання якої виходить за рамки геометричної оптики;
3) в однорідному середовищі промені світла розповсюджуються прямолінійно. На почкату 20 століття було відкрито явище огинання світлом перепон – дифракція.
4) закон відбивання світла: кут падіння світлового променю дорівнює куту його відбивання. Падаючий і відбитий промені і перпендикуляр, встановлений в точці падіння – лежать в одній площині.
5) закон Снеллиума: відношення синуса кута падіння до синусу кута – постійна для двох середовищ.

Геометрична оптика допускає викривлення променів світла в оптично неоднорідному середовищі.

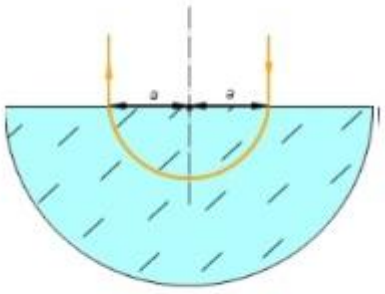

Рисунок 4.8 Розповсюдження в неоднорідних середовищах

На рисунку показник переломлення речовини в на півсфері залежить від відстані до її центру, по формулі $n=n_0/(1+(r/r_0)2)$. Промінь падаючий на відстань r_0 від центру на півсфери, вийде з іншої сторони на тій же відстані від центру.

Під час розповсюдження світла в напівпрозорому середовищі, наприклад склі, він рухається значно повільніше через неперервну взаємодію з атомами матеріального середовища. Якщо при перетині границь двох середовищ швидкість світла в другому середовищі нижча ніж швидкість світла в першій – промінь відхиляється в сторону перпендикулярної границі. Якщо в другому середовищі швидкість розповсюдження світла вище – промінь відхиляється на більший кут. Відношення швидкості світла в вакуумі до швидкості світла в просторі – коефіцієнт переломлення середовища. Коефіцієнт переломлення дорівнює приблизно 1,5, то світло в склі сповільнюється приблизно на третину в порівнянні з швидкістю его розповсюдження в вакуумі. Закон Снеллиума встановлює числові відношення між кутами падіння і переломлення променю при переході з одного середовища в інше. Сенс закону заключається в тому, що якщо відомі коефіцієнти переломлення світла в двух середовищах і кут падіння

променя, можна розрахувати на скільки він відхилиться після перетину границь між середовищами.

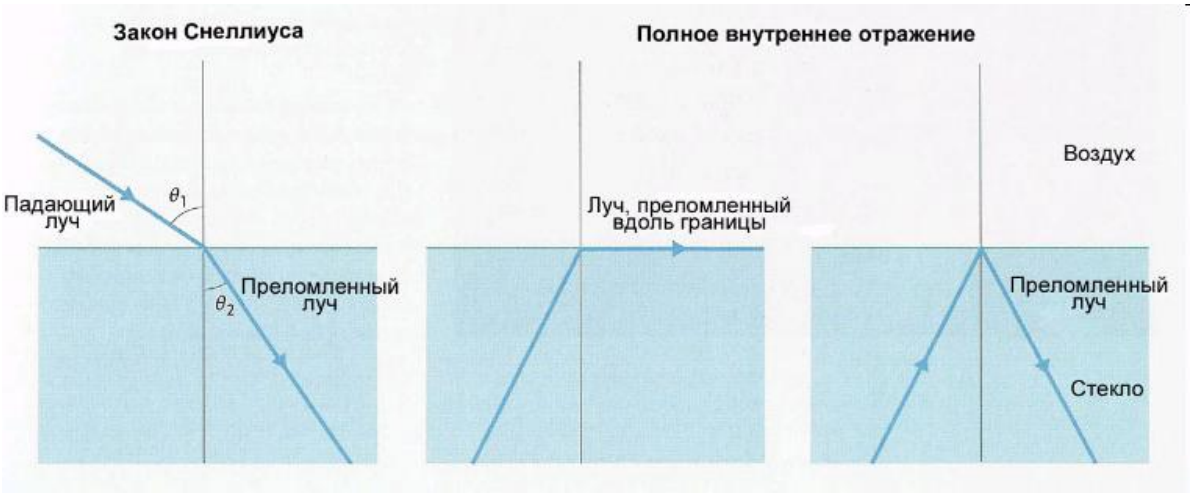

Рисунок 4.9 Переломлення світла в різних середовищах

Коефіцієнт переломлення дорівнює відношенню швидкостям розповсюдження світла в двох середовищах. $n=c_1/c_2$. Під час переходу променю з середовища оптично менш щільного в середовище більш щільне, переломлений промінь відхиляється ($n< 1$. При цьому існує граничний рівень $\beta = 90^o$ при деякому куті α. Ящко α перевищує це значення, то настає повне віддзеркалення. Кут переломлення більше 90^o означає, що промінь не вийде за границі скла і залишиться всередині тобто не переломиться, а віддзеркалиться від границі скла з повітрям. Це явище називають повним внутрішнім віддзеркаленням. Критичний кут визначається з рівняння: $\sin \theta > n2/n1$. Для передачі інформації мало просто створити світлову хвилю, її потрібно зберегти і направити в потрібне русло. В однорідному середовищі світло розповсюджується прямолінійно, але на границі зміни щільності середовища по оптичним законам проходить зміна направлення (віддзеркалення) або переломлення.

4.3. Види детектування оптичного сигналу

Детектування світла - нелінійне перетворення оптичного випромінювання видимого і інфрачервоного діапазонів частот (10^{15}-10^{13} Гц) в електричний сигнал у вигляді послідовності імпульсів або коливань струму радіочастотного діапазону. Цей сигнал несе інформацію про параметри оптичного випромінювання (інтенсивності, фазі, частоті). Детектування світла здійснюють за допомогою фотоприймачів (фотодіодів, фоторезисторів, фотопомножувачів), для яких характерна нелінійна (квадратична) залежність струму від напруженості E_c електричного поля світлової хвилі. Детектування світла застосовується в системах оптичного зв'язку, оптичної локації, оптичної обробки інформації, а також в спектроскопії, інтерферометрії, голографії та інші [11]. Основними різновидами детектування світла є пряме детектування і гетеродінірованія.

Пряме детектування. При прямому детектуванні світла на фотокатод приймача надходить корисний сигнал разом з фоновим випромінюванням. Для підвищення рівня сигналу щодо фону перед приймачем іноді поміщають смуговий оптичний фільтр і підсилювач. В результаті прямого детектування зміни інтенсивності випромінювання, всереднені за часом t і по площі фотокатода приймача, перетворюються в зміни потужності вихідного електричного сигналу. В силу статистичного характеру фотоемісії з катода утворюється дробовий шум (фотонний), який складається з шуму фонового випромінювання, шуму струму, що генерується всередині приймача, і з тепловим шумом навантаження. Ці шуми обмежують чутливість пристроїв детектування світла. Для виділення інформативних параметрів з дробовим і тепловим шумом вихідний електричний сигнал з приймача подається на оброблювальний пристрій, наприклад фільтр низьких частот (НЧ). Пристрої прямого детектування нечутливі ні до частоти, ні до фази, ні до кута падіння на

фотокатод несучою оптичної хвилі. Інформативним параметром при прямому детектуванні світла є тільки амплітудна модуляція прийому хвилі. Ефективність пристроїв детектування світла оцінюють величиною відношення сигнал / шум. Величина відношення сигнал/шум, так само як і величина середнього струму на виході приймача, не залежить від ступеня просторової когерентності випромінювання, що приймається. При реєстрації слабких світлових сигналів часто використовують метод фотоотсчётов (метод рахунку окремих фотонів)

Детектування неперервного оптичного сигналу. Вимір квадратурного компонента поля в сучасній оптиці виконується за допомогою техніки балансного гомоденування. Вона складається з змішанні вимірювального поля з інтенсивним опорним лазерним пучком на напівпропускаючому дзеркалі і подальшим виміром двох пучків за допомогою прямого детектування (вимірювання). Різність значення струмів двох детекторів дає виміряне значення квадратурної компоненти X (якщо фаза опорного пучка дорівнює 0) або Y (якщо фаза опорного пучка дорівнює $\pi/2$). Фаза опорного пучка повинна бути погоджена з фазою сигналу, опорний лазерний пучкой повинен бути частиною того випромінювання, яке генерує Аліса. Аліса ділить випромінювання лазера на дві нерівні частини, менша – модулюється і виконує роль сигналу, а більша – служить полем опорного пучка і відправляється Бобу по окремому квантовому каналу. Перехват Еви опорного сигналу не піддає схему КРК додатковій небезпеці, тому що при аналізі захищеності протоколу передбачається, що Ева може мати ту ж саму фазу, яку мають Аліса і Боб.

В описаній схемі балансного гомоденування використовуються недорогі фотодіоди на основі кремінь або арсеніда галію, працюючі в неперервному режимі.

Гетеродинування. Прилади детектування світла, які працюють по принципу гетеродинування, приймаючі оптичне випромінювання $E_c(t)$

комбінується на фотокатоді з опорним випромінюванням $E_{оп}(t)$. Результуюче поле на фотокатоді $E(t)=E_c(t)+ E_{оп}(t)$, а також струм I приймача пропорційний E_2 і має змінну, на різностній частоті [18]. Під час гетеродинному прийомі змінна вихідного сигналу несе інформацію не тільки про амплітуду приймаючого сигналу, а про частоту і фазу, якщо відома частота і фаза опорного випромінювання. Ефективність гетеродинування залежить від ступеню когерентності сигнального і опорного випромінювання і степені поєднання їх хвильових фронтів. Для ефективного гетеродинування необхідно виконувати вимоги на просторове погодження двох хвиль на поверхні фотокатода, яке вище від того чим менша довжина хвилі випромінювання. Гетеродинування широко використовується і дає можливість виділяти дуже слабкі сигнали.

Можливість гетеродинування світла була запропонована в 1947 ріці Г. С. Гореликом і експериментально реалізована американським фізиком А. Т. Форрестером.

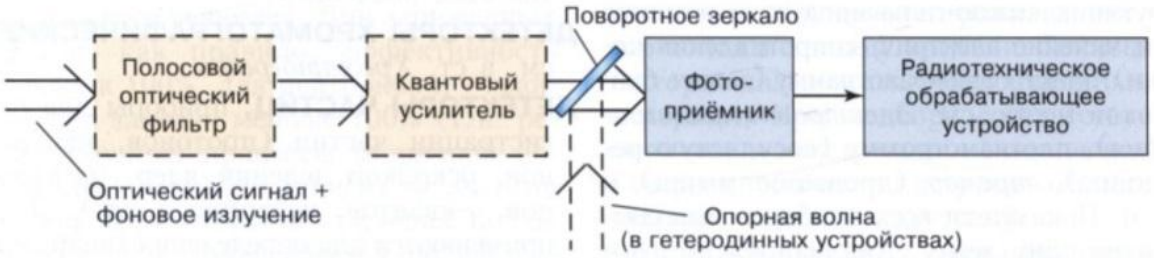

Рисунок 4.10 Схема гетеродинного детектування світла

Гетеродинування за допомогою лазерів. Високий рівень когерентності, монохроматичності і направленість лазерного випромінювання дозволяють отримувати високу ефективність гетеродинування з надвисоким розширенням вихідного сигналу, що важливо в спектроскопії розсіяного випромінювання. В гетеродинних спектрометрах розсіяне на наступному зразку лазерного випромінювання змішується з опорним, в якості якого зазвичай слугує бо частина випромінювання зондую чого лазера або випромінювання іншого

гетеродинного лазера. Відносно розширення такого спектрометру складає 10^8-10^{14} в залежності від тілесного куда збору розсіяного випромінювання.

У гетеродинних системах лазерного зв'язку і гетеродинних інтерферометрах інтенсивності, що застосовуються в астрономічних спостереженнях, використовують інфрачервоне випромінювання з довжиною хвилі 10 мкм. У цьому діапазоні є вікно прозорості і менше спотворення, що вносяться турбулентної атмосферою.

Якщо частота реєстрованого випромінювання збігається з частотою опорного випромінювання, то таке детектування називають гомодинним. Балансове гомодинне детектування світла використовують для реєстрації некласичного квадратурного-стисненого світла.

Розробляються принципово нові методи лазерного детектування світла, основані на використанні зв`язаних електронів. Це робить можливим детектування слабких оптичних сигналів без фотовідліків, тобто при подавлених дробових шумах.

4.4. Схеми перехоплення інформації

Найбільш простою і реалізуємою схемою перехоплення – заміна шумного квантового каналу на менш шумний і відведення частини сигнального пучка за допомогою частково прозорого скла з наступним гомодинним виміром тієї квадратурної компоненти, яку вибрав Боб. Внаслідок того що дзеркало вносить в канал лінійні втрати, то така атака не відрізняється від природного затухання світла в оптоволокні або відкритому середовищі [19]. При цьому частини одого і того ж багато фотонного імпульса потрапляють до Боба і Еви, на відмінну від однофотонних схем КРК, де така можливість є тільки в порівняному рідкісному випадку присутності декількох фотонів в одному імпульсі. Така атака належить

до типу індивідуальних непрямих атак. Інші типи атак не обговорюються, внаслідок неможливості їх продуктивної реалізації.

Висновок до розділу 4

В якості джерел когерентних станів використовується стабілізований по частоті і фазі лазер, який може працювати в неперервному стані. В останніх експериментах в одному імпульсі випромінювання лазері було приблизно 250 фотонів. Кожен імпульс переносить один символ в ключі.

Середовище передачі сигналу – оптичне волокно або відкрите середовище. Методи КРК в яких взято за основу когерентні стані малочутливі до флуктацій поляризації і втратам. В залежності від середовища передачі, в напівпрозорому середовищі сигнал буде рухатись повільніше ніж в прозорому, через взаємодію атомів.

Під час детектування оптичного сигналу може використовуватись декель методів. Якість детектування напряму залежить від матеріалі з яких виготовлено детектор.

Всі відомі схеми перехоплення інформації приносять мало результативні, алі найбільш небезпечним є схема підміни стороннім користувачем каналу, який є менш зашумленим, ніж реальний канал. Такий спосіб атаки відноситься до індивідуальних непрямих.

РОЗДІЛ 5. ЗОНДУВАННЯ МЕРЕЖІ ЗА ДОПОМОГОЮ ЗАПЛУТАНИХ ФОТОНІВ

5.1. Блок-схема приладу та опис складових приладу

Прилад зоднування лінії зв'язку на основі віддзеркалення сигналу назад до відправника.

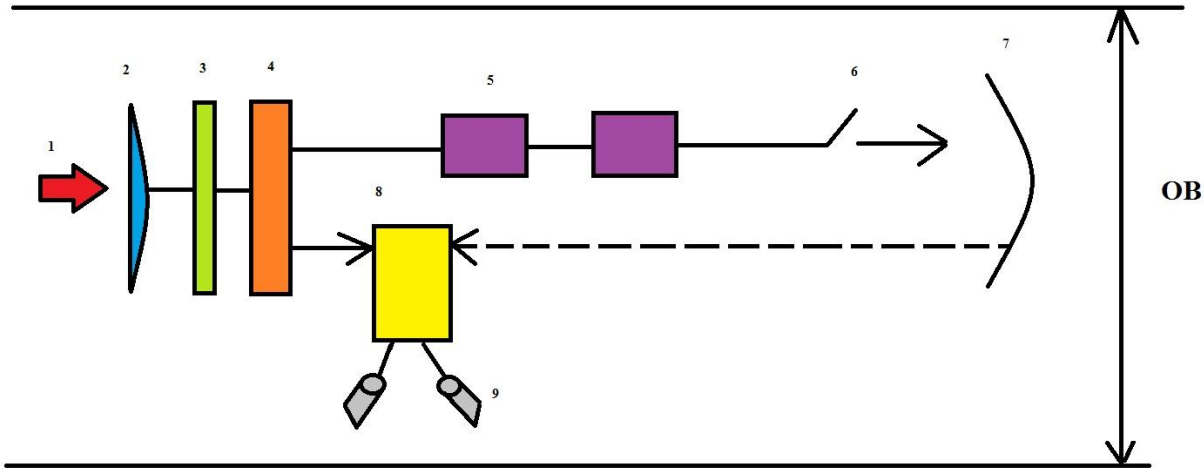

Рисунок 5.1 Блок-схема квантового рефлектометра.

1 – лазер; 2 – лінзи; 3 – коліматор; 5 – комірки Поккельса; 6 – керований електричний перемикач; 7 – параболічне дзеркало; 8 – кальцитна призма; 9 – фотоелектронний помножувач (ФЕП).

Лазер. Представляє собою оптичний квантовий генератор – прилад випромінюючий вузький пучок світла. Надає можливості передачі енергії на будь-які відстані зі швидкістю світла. Звичайне світло, яке дають різноманітні джерела можна характеризувати, як невеликі пучки світла, які розлітаються в різних напрямках. Їх можно концентрувати за допомогою вігнутого дзеркала або лінзи.

Лазерний промінь складається з квантових частинок світла, які породжуються шляхом примусової активації фотонів прозорого середовища, що є основою лазерного випромінювання. Для того щоб викликати лавиноподібне випромінювання в рубіновому стержні, потрібно подіяти (вдарити) на атоми енергією іншого джерела, наприклад, світлом яке породжується під час вибуху. Вдаряючись з речовиною рубіна кожен зовнішній фотон вибиває з його атомів новий фотон, який буде рухатись з тією ж силую і направленням, і зіштовхнувшись з новим атомним ядром вибиває нову частинку світла. Завдяки полірованості стінок рубіна, діючі як відзеркалюючі дзеркала, потік фотонів багато разів проходить цей шлях, поки не досягне великої щільності. Нахил дзеркальної поверхні може бути змінено і промінь великої енергетичної потужності вилетить назовні. Щоб досягти випускання лазерного випромінювання, необхідного до робочої речовини ввімкнути джерело енергії, яке викликає збудження фотонів – накачка.

Волоконні лазери. Середовище – оптичне волокно, накачка – широкосмугові світлодіоди. Оптичне волокно виготовляється з кварцу, високий коефіцієнт прозорості забезпечую насичення станів енергетичніх рівніх атомів. Домішки, які додаються в кварц роблять його поглинаючим середовищем сторюючи неоднорідний стан заселеності енергетичних рівнів при вибраній потужності накачки. Мають високі показники випромінювання та невеликі розміри, вмонтовуються в волоконні лінії.

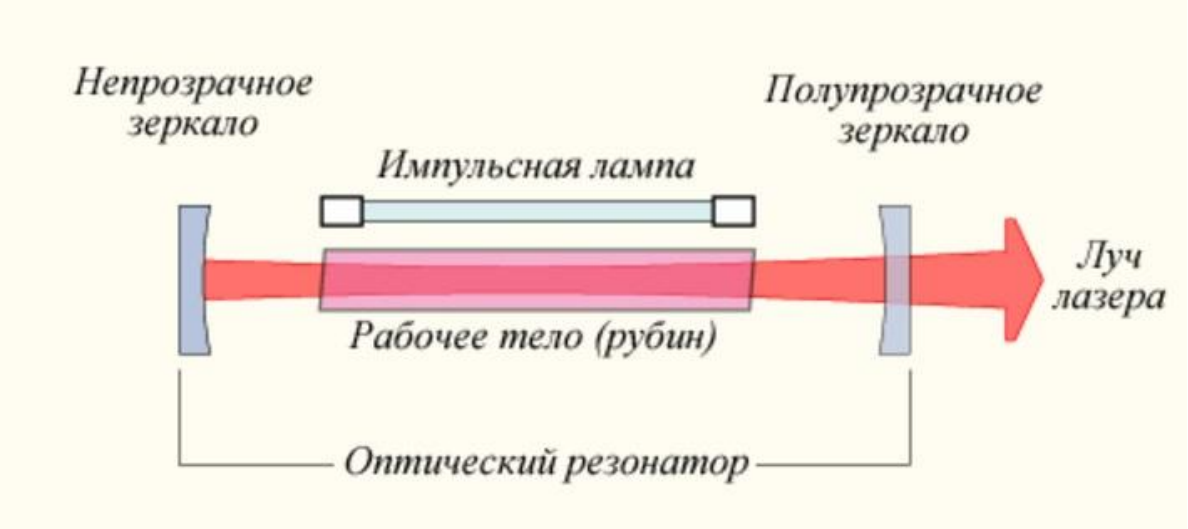

Рисунок 5.2 Рубіновий лазер

Застосування лазерів. Випромінювання лазера має унікальні властивості, які знайшли місце в різних галузях науки і техніки. Ексимерні лазери – в медицині для хірургічного лікування. Волоконні – різка металів, маркування, квантової передачі в лінії, тощо. Також широко використовуються в інформаційних технологіях.

Лінзи. Лінзи зазвичай мають сферичну або близьку до сферичної поверхню. Можуть бути увігнутими та випуклими або плоскими. Маючи дві поверхні, через які проходить світло, вони можуть по-різному поєднуватись, утворюючи різні види лінз:

- Якщо дві поверхні випуклі, центральна частина товще, ніж по краям;
- Лінза з випоклую і увігнутою сферами називається меніском;
- Лінза з однією плоскою поверхнею моє назву плоско-увігнутою або плоско-випуклою, в залежності від другої сфери.

Незалежно від поєднання поверхностей, якщо їх товщина в центральній частині більше ніж по края, такі лізни називаються збираючими. Мають позитивну фокусну відстань. Розрізняють види лінз:

- Плоско-випуклі;
- Двояковипуклі;
- Увігнуто-випуклі (меніск).

Якщо товщина в центрі менше ніж по краям, то такі лізни мають назву розсіювальні. Вони мають від'ємну фокусну відстань. Види розсіювальних лінз:

- Плоско-увігнуті;
- Двоякоувігнуті;
- Випукло-увігнуті.

Промені від точкого джерела розходяться з одніє точки, їх називають пучком. Коли пучок входить в лінзу, кожен промінь переловлюється змінючи своє направлення. Саме за цього пучок може вийти з лінзи і більшій або меншій мірі розбіжним.

Точковий пучок джерела світла називається дійним об'єктом, а точка сходи мості пучка променій, яка виходить з лінзи є його дійсним зображенням. Важливе значення має масив точкових джерел, розподілених на плоскій поверхні, прикладом може бути матове скло.

Точки на площині зображення 1:1 відповідають точкам на площині об'єкта. Так само це відноситься до геометричних фігур, хоча отримана картинка може бути перевернутою по відношенню до об'єкта, зверху вниз або зліва направо. Сходження променів в одній точці створюю дійсне зображення, а розбіжне – уявне. Коли воно чітко окреслене на єкрані – дає дійсне зображення. Ящко зображення можна побачити тільки через дивлячись через лінзу в сторону джерела світла - називається уявним. Проекція об'єктива камери на плівку дає дійсне зображення.

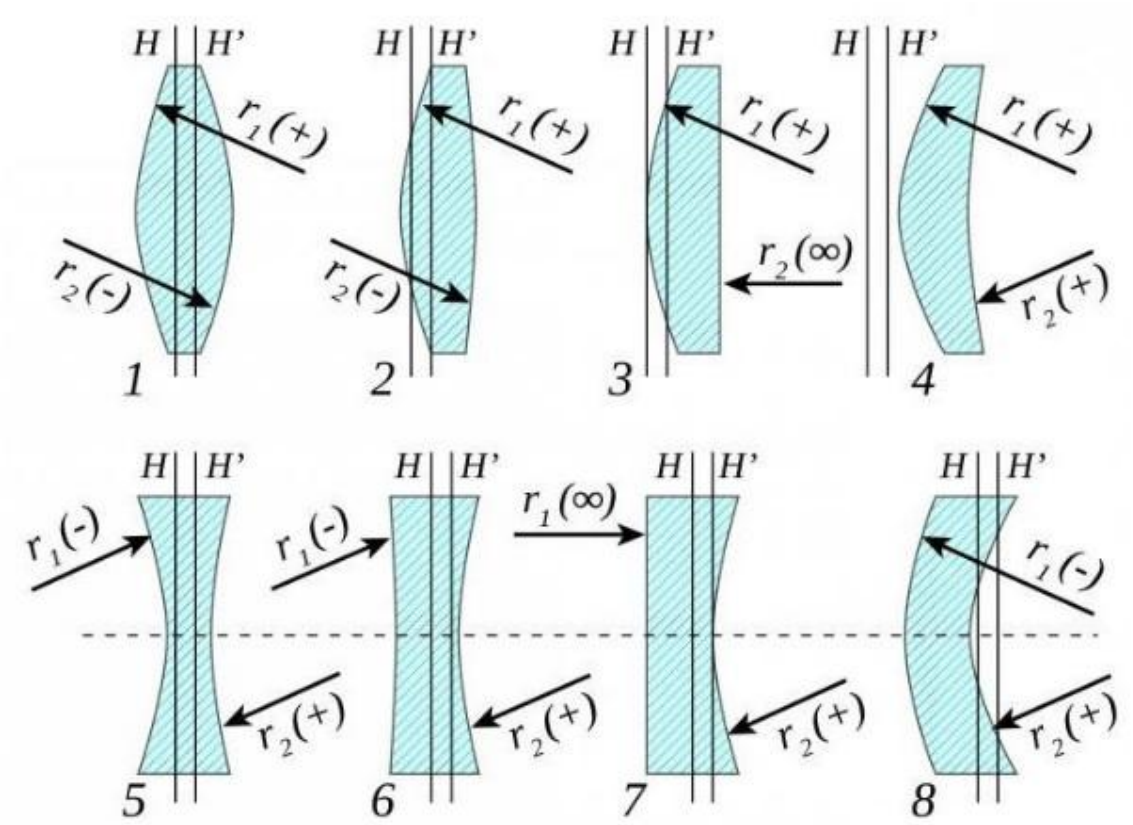

Рисунок 5.3 Приклади переломлення променів

Фокус лізни можна знайти пропустивши через неї пучок паралельних променів. Точка в якій вони зійдуться – її фокус F. Відстань фокальної точки до об’єктива називають фокусною відстанню f. Паралельні промені можна пропустити з двох сторін і знайти таким чином два фокуси F. Кожна лінза має два F і два f. Ящко вона відносно тонка порівняно з її фокусною відстанню, то останні приблизно рівні.

Позитивною фокусною відстанню характеризуються збираючі лінзи. Лінзи такого типу зводять промені, які в них входять. Збираючі об’єктиви можут формувати дійсне і уявне зображення. Перше формується в випадку, ящко відстань від лінзи до об’єкта перевищую фокусне.

Від’ємними фокусними відстанями характеризуються розсіювальні лінзи. Лінзи такого типу розводять промені більше, нід вони були розведені до

моменту попадання на їх поверхню. Розсіювальні лінзи створюють уявне зображення.

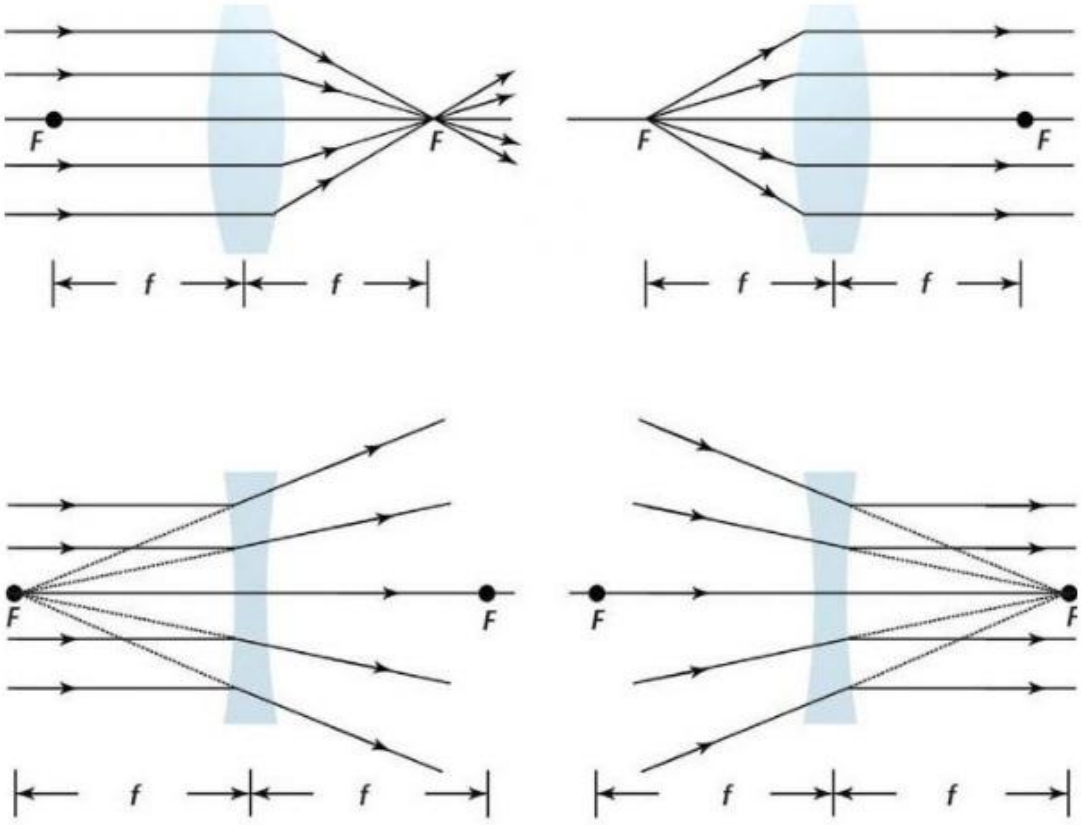

Рисунок 5.4 Розсіювання та збирання променів проходячих через лінзу

Коліматор. Приклад для отримання паралельних променів світла або частинок.

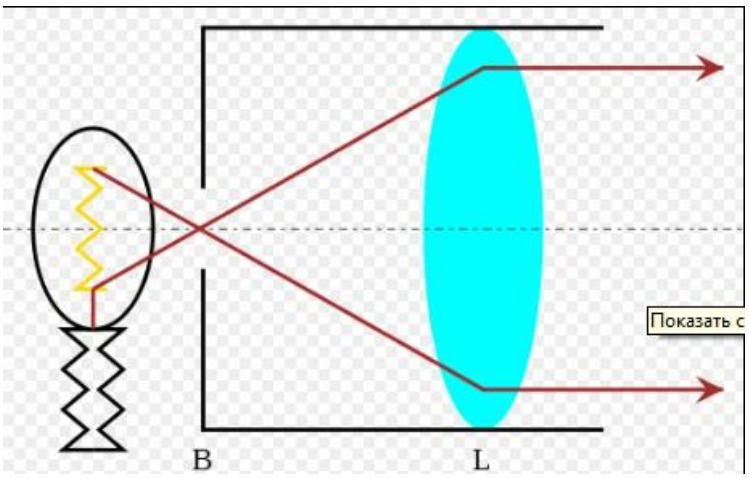

Рисунок 5.5 Схема простого коліматора

Оптичний коліматор. Приклад для отримання паралельних світлових променів. Складається з об’єктиву, в фокальній площині якого розміщено джерело світла малої величини. Найчастіше таким служить отвір не прозорої діафрагми, наприклад візулький отвір постійноє або змінної ширини. Відносне розміщення об’єктива і джерела фокусується закріпленням їх в корпусі. Не прозорі всередині стінки коруса поглинають промені, направлення яких не співвпадає з оптичної віссю об’єктива. Не ідеальність паралельного пучка, який виходть з коліматора обумовлена кінцевим розміром джерела і аберація ми об’єктива.

Коліматор частинок. Являють собою довгий отвір з формою поперечного перерізу, зроблене в поглинаючому матеріалі. На одному з кінців коліматора знаходится джерело випромінювання. Найпростіші з таких коліматорів застосовуються в оптиці. Коли необхідно отримати лплоский пучок, застосовуються отворні коліматори, в такому випадку квазіпаралельними є тільки проекції променів на площину перпендикулярну пропилі отвору.

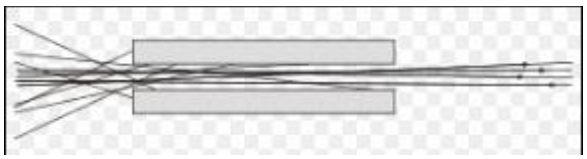

Рисунок 5.6 Коліматор частинок

Поляризатор. Прилад призначений для отримання повністю частково поляризованого птичного випромінювання з випромінювання в довільному стані поляризації. Відповідно з типом поляризації, поділяються на лінійні і кругові. Лінійні поляризатори дозволяють отримати плоскополяризоване світло, а кругові – поляризоване світло по колу.

Лінійні поляризаторі основані на використовувані:

- Подвійному переломленні променя;

- Лінійний діхроізм;
- Поляризація світла при вдзеркаленні на границі розділу середовищ.

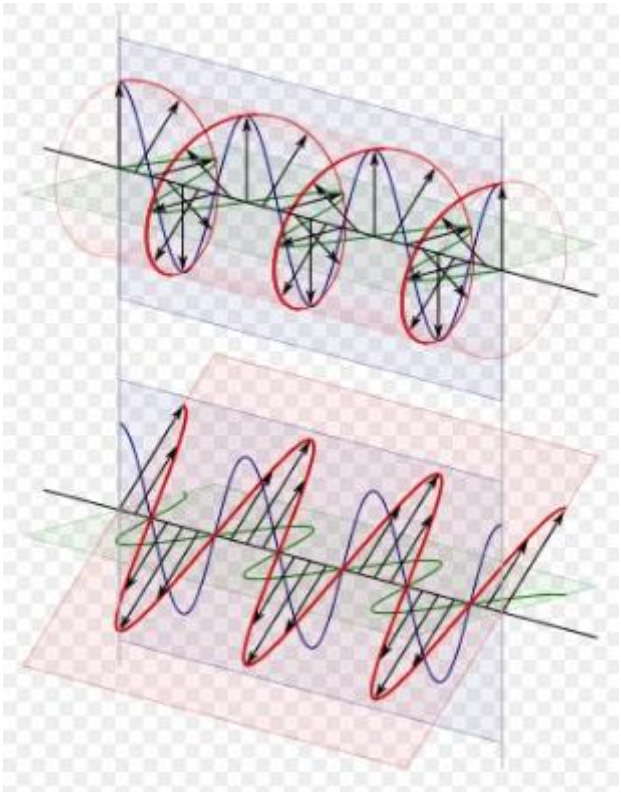

Рисунок 5.7 Кругова і плоска поляризації

Комірки Поккельса. Ефект Поккельса – явище виникнення подвійного переломлення променів в оптичному середовищі, яке виникає під час накладання постійного чи змінного електричного поля. Ефект можна спостерігати в кристалах, які не мають центру симетрії, в силу лінійності при зміні направлення поля ефект повинен змінювати знак, що не є можливим в центрально-симетричних тілах. Ефект можна спостерігати в кристалах ніобата літія і арсеніда галія. Цей ефект був відкритий в 1893 році і названий в честь Ф. Поккельса, який вивчан це явище.

Електричний перемикач. Електромеханічний пристрій для розмикання електричного струму з одного провідника на інший. Призначений для зміни з’єднання в одному або кількох електричних колах. Перемикачі можут кируватись автоматично вихідними сигналами сенсорів, чутливих температури, тиску, положення або світла. В ідеальних умовах на контакт не потрапляє напруга, коли він замкнутий і немає обмежень по величині струму і напруги. Наростання і падіння проходить миттєво без збоїв. На практиці контакти перемикачів мають опір, обмежені по струму на напрузі. Такі відхилення враховуються при розрахунках розгалужених мереж з великою кількістю перемикачів.

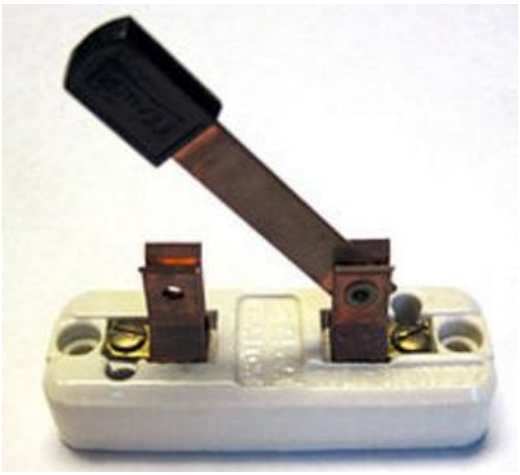

Рисунок 5.8 Перемикач

Параболічне дзеркало. Пристрій відзеркалююча поверхя якого маю вигляд параболи. Параболічне дзеркало може бути випуклим або вігнутим, в залежності яка стороні буду відзеркалюючою. Центр відповідає параболічному дзеркалу і називається його центром, середина сегменту – полюс дзеркала, пряма яка проходить через центр і полюс – оптична вісь.

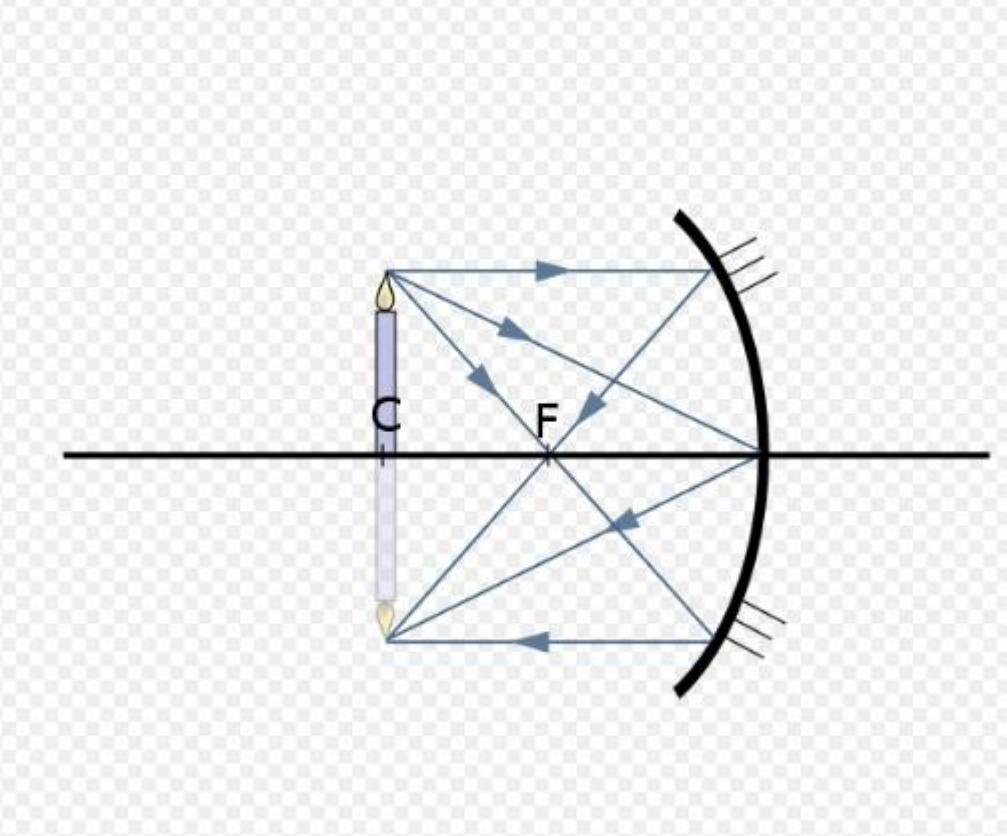

Рисунок 5.9 Параболічне дзеркало. Приклад Відзеркалення.

Кальцитна призма. Призма виготовлена на основі кальциту – біомінерал, завдяки своєм властимостій застосовується в систем передачі. В чистому стані не має забарвлення або білий. Широко використовується в будівництві та в хімічній промисловості. Ісландський шпат використовується в оптичних приладах. При проходженні променю через кальцитну призму розщеплю промінь під кутом 50-60°, після чого сигнал поступає на інший прилад (ФЕП), як зазначено на рисунку блок-схеми.

Фотоелектронний перемножував (ФЕП).

Електровакуумний пристрій, в якому потік фотонів випромінюваний фотокатодом під дією оптичного випромінювання підсилюється в перемножувальній системі, в результаті вторичної електронної емісії. Вперше був запропонований в 1930-1934 роках, винахідником Л. А. Кубецьким.

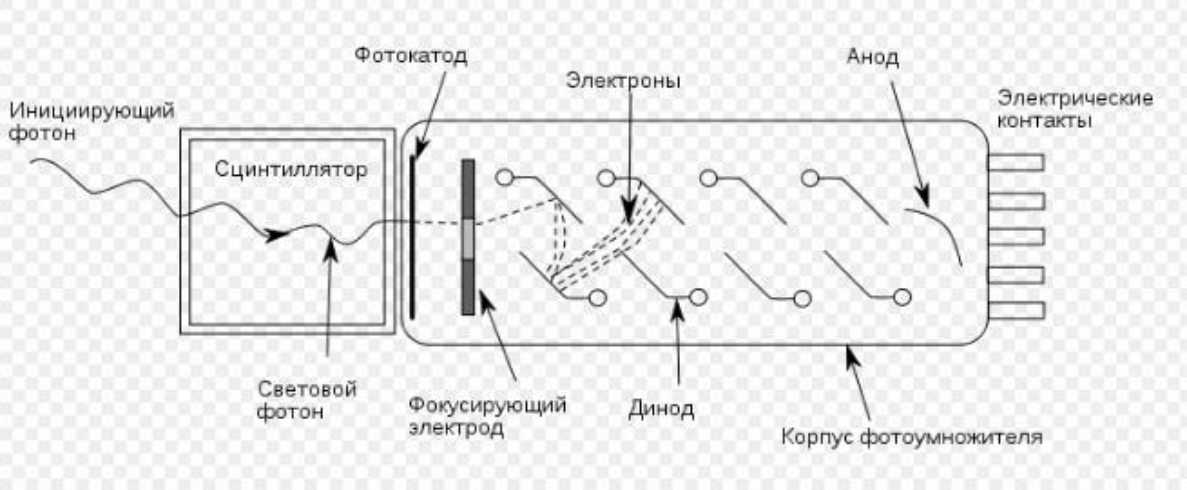

Рисунок 5.10 Схема ФЕП.

ФЕП складається з вхідної камери, перемножу вальної дінодної, анода і додаткових електродів. Елементи розміщуються в вакуумному корпусі. Поширені ФЕП ті, в яких підсилення потоку електронів створюється за допомогою спеціальних електродів зігнутоє форми – дінодів, коефіцієнт вторичної емісії яких більше 1. Для фокусування і прискорення електронів на анод і дінод подається напруга від 600 В до 3000 В. також використується магнітне фокусування. Також є ФЕП з напівпровідниковими перемножувальними елементами, принцип дії заснований на іонізації атомів напівпровідника і бомбардування його електронами.

5.2. Опис роботи приладу

Квантова заплутаність - явище, при якому квантові стани двох фотонів взаємопов'язані. Простіше кажучи, при деяких умовах можна отримувати пару фотонів одночасно, і вони будуть заплутаними. Так, наприклад, можна отримувати два фотона з протилежно спрямованими спинами в так званому синглетному стані. А якщо заміряти спін одного з них і він виявиться «+», то можна з упевненістю сказати що спін другого буде «-» або навпаки.

Спін квантової частинки (електрона або фотона) - це її внутнішній власний кутовий момент. Якщо рознести два заплутаних фотона в просторі, то фотони все одно будуть пов'язані один з одним. Наприклад, китайським вченим вдалося рознести заплутані фотони на відстань 1200 км і експериментально підтвердити факт заплутаності.

Для отримання заплутаних фотонів іноді служить нелінійний матеріал, на який направляється лазерний потік. В результаті розсіювання більш високо енергетичного фотона на виході отримуємо два або більше фотонів з більш низькою енергією, які являються заплутаними.

На даний момент існує кілька способів генерації коду, які забезпечують захист інформації від сторонніх осіб, наприклад, BB84, B91, B92. Всі вони вимагають наявності відкритого каналу зв'язку між передавачем і приймачем. Здійснити сканування каналу на предмет прослуховування можна простіше без наявності такого зв'язку, що істотно підвищить надійність роботи системи.

Для побудови пристрою на основі сканування лінії передачі нам знадобиться звичне середовище передачі заплутаних фотонів, а так само на приймальній стороні відбивач, наприклад, параболічне дзеркало, яке зможе повністю відобразити прийняті фотони назад в сторону відправника.

Опис роботи. Передавач формує один з двох станів поляризації - лазер, лінзи, коліматор. Ячейки Поккельса необхідні для імпульсної варіації поляризації потоку квантів передавачем і для аналізу імпульсів поляризації приймачем. Як лінію передачі використовується оптичне волокно. Один із заплутаних фотонів направляється в лінію, а другий – опорний - направляється на пристрій вимірювання поляризації. Як пристрої вимірювання поляризації використовуються кальцитові призми, які призначені для розщеплення пучка і два однофотонних детектора (наприклад ФЕП), призначені для детектування поляризованих фотонів.

За допомогою призм і ФЕП можна вимірювати дві ортогональні складові поляризації фотонів. На приймальній стороні лінії розташований електрично керований перемикач, що направляє заплутаний фотон на параболічне дзеркало яке відправляє їх назад на передавальну сторону, де опорний і передані фотони аналізуються (звіряються) по поляризації. Після підрахунку збігу поляризацій переданих та опорних фотонів можна зробити висновок було наявність "прослуховування" або воно відсутнє.

Якщо уявити що послідовне проходження фотоном кожного елемента пристрою проходить незалежно один від одного, то «сумарна» ймовірність будет дорівнювати добутку парціальних ймовірностей проходження послідовних елементів. Ящко можливі шляхи проходження фотона лежать паралельно, то ймовірність його проходження відповідно складається. Тепер, якщо уявити, що коефіцієнт передачі елемента (в разах) це ймовірність проходження фотона через прилад, ми по відомим значенням втрат (в разах) можемо розрахувати «сумарну» ймовірність проходження фотона і оцінити кількість втрачених і кількість фотонів, які пройшли, а також вимоги висунуті кожному елементу приладу заданої сумарної вірогідності проходження.

Затухання в кажному елементі схеми буде приблизно 0.1-0.2 дБ. Значення в децибелах переводимо в рази: $T=10^{(-S/10)}$, де S – коефіцієнт передачі по потужності в децибелах, а T – коефіцієнт передачі потужності в разах.

1) Лінзи $S_1=0.1$ дБ, $T_1=0.977$;
2) Коліматор $S_2=0.2$ дБ, $T_2=0.954$;
3) Поляризатор $S_3=0.1$ дБ, $T_3=0.977$;
4) Ячейки Поккельса $S_4=0.2$ дБ, $T_4=0.954$;
5) Параболічне дзеркало $S_5=0.1$ дБ, $T_5=0.977$;
6) Призма $S_6=0.2$ дБ, $T_6=0.954$;
7) ФЕП $S_7=0.2$ дБ, $T_7=0.954$.

Виходячи з того, що схема приладу послідновa всі отримані потужності (в разах) перемножуємо. $T=T_1 \cdot T_2 \cdot T_3 \cdot T_4 \cdot T_5 \cdot T_6 \cdot T_7=0.772$.

В результаті отримуємо приблизну ймовірність проходження фотону через прилад.

В майже ідеальному приладі показники елементів в кожному з приладів повинні мати значення по путужності 0.009 дБ, щоб на виході отримати 95-97% проходження фотону через прилад.

Висновок до розділу 5

В розділі описана робота та принцип дії приладу, який заснований на зондуванні лінії зв'язку заплутаними фотонами. Перевагою такого пристрою є те що до моменту відправки конфіденційно важливого повідомлення ми маємо змогу перевірить канал на предмет прослуховування. В кінці процесу запускання в лінію двох заплутаних фотонів, виконується підрахунок збігів поляризацій. Після перевірки лінії, в разі повного збігу, користувачі можут обмінюватись конфіденційною інформацію. Можуть бути різні варіації такої схеми з використанням заміни приладів на більш точні. Недоліком в такій схемі можут виступати використовувані прилади.

ВИСНОВКИ

1. В роботі було досліджено змішані стани, вони представляють собою комбінації двох або більше джерел, які породжують змішані стани з деякою вірогідністю ρ. Позитивний оператор ρ в гільбертовому просторі зі слідом 1, відповідає якомусь квантовому стану.
2. Оптична система призначена для перетворення поля випромінювання до оптичної системи, таке перетворення за допомогою явища інтерферації випромінювання.
3. Когерентні стани виділяються серед інших станів одномодових полів своєю унікальністю. Розподілення числа фотонів – ймовірність зареєструвати поле в стані з заданим числом фотонів.
4. Квантова переплутаність – передача стану одного фотона на інший без відправлення самого фотона.
5. Квантова криптографія – шифрування інформації різними методами, для забезпечення конфіденційності. Реальною загрозою для квантових систем передачі є маскування сторонніх осіб під природний шум який присутній в каналі зв’язку.
6. Широко використовуваний спосіб отримання одиночних фотонів – використання нелінійно-оптичного процесу спонтанний параметричний розпад. Для детектування одиночних фотонів використовують такі прилади: ЛФД, ФЕП, гарячі електронні балометри, сенсори граничного переходу, квантові точки.
7. Середовищем розповсюдження сигналів є оптичне волокно і відкрите середовище. Детектування неперервного оптичного сигнула відбувається за допомогою балансного гомоденіювання.
8. Під час вивчення матеріалу було запропоновано створення приладу, який дозводить перевірити наявність прослуховування в лінії. Після

зондування лінії заплутаними фотонами і перевірки збігів поляризації, можна зробити висновок чи було наявне в лінії прослуховування.

ПЕРЕЛІК ПОСИЛАНЬ

1. Жиров О.А. Квантовая механика, Новосибирск, 2003. – 76 с. Смешанное состояние квантовых систем – стр. 15 – 16.

2. *Березин Ф. А., Шубин М. А.* Уравнение Шредингера.— М.: Изд-во МГУ.— 1983.— 392 с.

3. С.Я.Килин, Д.Б.Хорошко, А.П.Низовцев Квантовая криптография. - Минск: Белорусская наука, 2007. - 391 с.

4. Скалли М.О., Зубайри М.С. Квантовая оптика. М.:ФИЗМАТЛИТ, 2003 г.

5. Bell, J. On the Einstein Podolsky Rosen paradox / J. Bell //Physics.— 1964.— Vol. 1.— P. 195–200.

6. Харин, Ю. С. Математические основы криптологии / Ю. С. Харин, В. И. Берник, Г. В. Матвеев.— Минск: БГУ, 1999.

7. Bennett, C. H. Quantum cryptography: Public key distribution and coin tossing / C. H. Bennett, G. Brassard // Proceedings of IEEE International Conference on Computers and Systems and Signal Processing (Bangalore, India). —1984.— P. 175–179.

8. Bennett, C. H. Quantum cryptography using any two nonorthogonal states / C. H. Bennett // Phys. Rev. Lett. — 1992.— Vol. 68.— P. 3121.

9. Ekert, A. Quantum cryptography based on Bell's theorem / A. Ekert // Phys. Rev. Lett. — 1991.— Vol. 67, № 6. — P. 661–663.

10. Basche, T. Photon antibunching in the fluorescence of a single dye molecule trapped in a solid / T. Basche, W. E. Moerner, M. Orrit, H. Talon // Phys. Rev. Lett. — 1992.— Vol. 69.— P. 1516–1519.

11. Килин, С. Я. Квантовая оптика: поля и их детектирование / С. Я. Килин.— Минск: Наука и техника, 1990; М.: Едиториал УРСС, 2003.

12. Берковский А. Г., Гаванин В. А., Зайдель И. Н., Вакуумные фотоэлектронные приборы, 2 изд., М.

13. Gisin, N. Towards practical and fast quantum

cryptography / N. Gisin, G. Ribordy, H. Zbinden et al. // arXiv:quant-ph/0411022.— 2004.

14. Ekert, A. K. Practical quantum cryptography based on two-photon interferometry / A. K. Ekert, J. G. Rarity, P. R. Tapster, G. M. Palma // Phys. Rev. Lett. — 1992.— Vol. 69.— P. 1293.

15. Muller, A. “Plug and play” systems for quantum cryptography / A. Muller, T. Herzog, B. Huttner et al. // Appl. Phys. Lett. — 1997.— Vol. 70.— P. 793.

16. Fuchs, C. A. Optimal eavesdropping in quantum cryptography. I. information bound and optimal strategy / C. A. Fuchs, N. Gisin, R. B. Griffiths et al. // Phys. Rev. A. — 1997.— Vol. 56, № 2.— P. 1163–1172.

17. Hirano, T. Quantum cryptography using pulsed homodyne detection / T. Hirano, H. Yamanaka, M. Ashikaga et al. // Phys. Rev. A. — 2003.— Vol. 68.— P. 042331.

18. Lorenz, S. Continuous variable quantum key distribution using polarization encoding and post selection / S. Lorenz, N. Korolkova, G. Leuchs // Appl. Phys. B. — 2004.— Vol. 79.— P. 273.

19. Grosshans, F. Continuous variable quantum cryptography / F. Grosshans, P. Grangier // Phys. Rev. Lett. — 2002.— Vol. 88, № 5.— P. 057902.

20. Тычинский В.П. Мощные газовые лазеры, УФН, т. 91, вып. 3, 1967, стр. 389 – 424.